1988-03

Design of Defense Data Network for the Republic of Korea military

Lee, Kyoo Won.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/23166

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DESIGN OF DEFENSE DATA NETWORK FOR THE REPUBLIC OF KOREA MILITARY

by

Lee, Kyoo Won

March 1988

Thesis Advisor Judith H. Lind

Approved for public release; distribution is unlimited.

Unclassified

security classification of this page

REPORT DOCUMENTATION PAGE

1a Report Security Classification Unclassified	1b Restrictive Markings
2a Security Classification Authority 2b Declassification Downgrading Schedule	3 Distribution Availability of Report Approved for public release: distribution is unlimited.
4 Performing Organization Report Number(s)	5 Monitoring Organization Report Number(s)
6a Name of Performing Organization Naval Postgraduate School | 6b Office Symbol *(if applicable)* 62	7a Name of Monitoring Organization Naval Postgraduate School
6c Address *(city, state, and ZIP code)* Monterey, CA 93943-5000	7b Address *(city, state, and ZIP code)* Monterey, CA 93943-5000
8a Name of Funding Sponsoring Organization | 8b Office Symbol *(if applicable)*	9 Procurement Instrument Identification Number
8c Address *(city, state, and ZIP code)*	10 Source of Funding Numbers Program Element No | Project No | Task No | Work Unit Accession No

11 Title *(include security classification)* DESIGN OF DEFENSE DATA NETWORK FOR THE REPUBLIC OF KOREA MILITARY (Unclassified)

12 Personal Author(s)
Lee, Kyoo Won

13a Type of Report Master's Thesis	13b Time Covered From To	14 Date of Report *(year, month, day)* 1988 March	15 Page Count 75

16 Supplementary Notation The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 Cosati Codes

Field	Group	Subgroup

18 Subject Terms *(continue on reverse if necessary and identify by block number)*
Data Communications, Defense Data Network

19 Abstract *(continue on reverse if necessary and identify by block number)*

This thesis provides the concepts for the construction of an integrated computer communications network, as would be appropriate for the Republic of Korea (ROK) Defense Data Network (DDN). The current ROK military communications system and its problems are discussed, along with the requirements of the ROK Armed Forces. The basic concepts of data communications and the United States DDN are also analyzed. Through synthesis of these concepts, the goals of the required system and a proposed ROKM DDN model are provided.

20 Distribution Availability of Abstract ☒ unclassified unlimited □ same as report □ DTIC users	21 Abstract Security Classification Unclassified	
22a Name of Responsible Individual Judith H. Lind	22b Telephone *(include Area code)* (408) 646-2543	22c Office Symbol 55Li

83 APR edition may be used until exhausted
All other editions are obsolete

security classification of this page

Unclassified

Design of Defense Data Network for the Republic of Korea Military

by

Lee, Kyoo Won
Captain, Republic of Korea Army
B.S., Korea Military Academy, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS
MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1988

ABSTRACT

This thesis provides the concepts for the construction of an integrated computer communications network, as would be appropriate for the Republic of Korea (ROK) Defense Data Network (DDN). The current ROK military communications system and its problems are discussed, along with the requirements of the ROK Armed Forces. The basic concepts of data communications and the United States DDN are also analyzed. Through synthesis of these concepts, the goals of the required system and a proposed ROKM DDN model are provided.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

A. BACKGROUND

The need for data communications has grown greatly in recent years. Computer and communications technology has also advanced rapidly. Communications systems play an important role in national defense, which is essential to all the countries in the world, including Korea.

The peninsula known as Korea was divided into two parts after World War II. These are the Republic of Korea (ROK) and North Korea. North Korea is very aggressive and has powerful military forces. In order to defend itself, ROK also has large Armed Forces--Army, Navy, and Air Force.

Each of the ROK Armed Forces presently has its own communications system, and operates it separately. However, it is critical that data and information be exchanged rapidly and accurately among all of the Armed Forces. An integrated communications system is needed greatly.

B. PURPOSE

As stated before, although the various Forces of the ROK Military (ROKM) have communications systems, there are no connections among these systems. The military urgently needs an integrated communications system, and a means to operate it efficiently. Consequently, the purpose of this thesis is to provide a strategy for the design and implementation of a ROKM integrated data communications system.

C. SCOPE

This thesis will identify and develop the specific design issues associated with a data communications network. It will also discuss the system analysis and requirements for the construction of a ROKM DDN. Since the goal is to design an efficient ROKM DDN, the current ROKM communications system problems and requirements will be analyzed. Data communications principles will be provided, and the United States (US) DDN will be described as a possible model for the ROKM DDN.

D. ORGANIZATION

This report contains six main chapters followed by a conclusions chapter. Chapter I provides a brief introduction, defining the research objective and its associated scope of effort, and outlines the organization of this thesis. Chapter II provides an introduction to ROKM communications system. Its problems and requirements are also discussed in this chapter. In Chapter III, the current aspects of US DDN are discussed. The basic concepts of data communications are discussed in Chapter IV.

The requirements of the ROKM communications system, which were discussed in Chapter II, and the ROKM DDN objectives and goals are developed in Chapter V. Chapter VI is devoted to the design of ROKM DDN model. In this chapter, the goals of the ROKM communications system will be applied to the model, along with strengths of the US DDN. The paper concludes with Chapter VII, where the summary of this thesis and the implementation strategy for a ROKM integrated data communications system will be provided.

II. THE ROKM COMMUNICATIONS SYSTEM

A. BACKGROUND

During the Korean War (1950-1953), the ROKM became very large. Moreover, the ROK needed even bigger and stronger Armed Forces after that war, in order to defend itself. As a result, the ROK has big and powerful Armed Forces, even though it is a relatively small country.

Under the Department of Defense (DOD), there are three military headquarters--Army, Navy, and Air Force. The relationships among these are shown in Figure 2.1. In general, the organization of the DOD and the three services is patterned closely after the US military system.

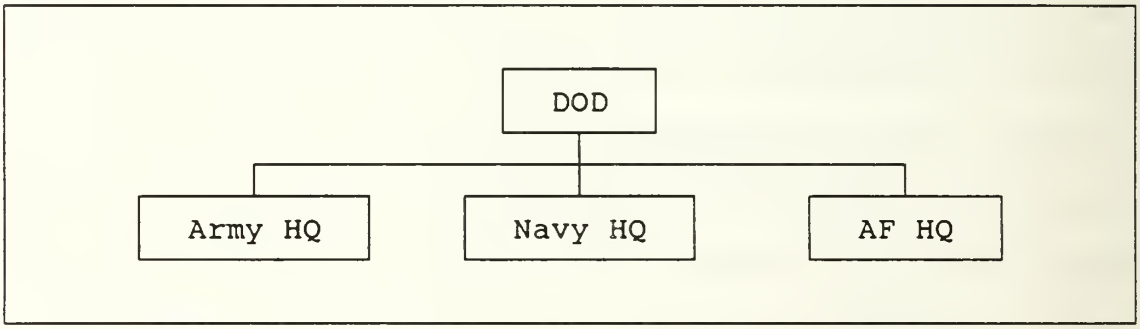


Figure 2.1 Structure of the ROKM

B. PRESENT ROKM COMMUNICATIONS SYSTEM

From the beginning of ROKM history, there have been no common communications channels among the Armed Forces. Each has developed its own communications system separately. Therefore, it is very difficult for a military unit to communicate with another Armed Force subunit.

ROKM has no data communications network like the well-developed US DDN. Communications takes place using telephones, radios, messengers, etc. Because the ROKM realizes that a common data communications network is necessary, it is trying to improve its communications system. For instance, by 1985 a computer system was assigned to each Army division headquarters. However, these systems use existing communications channels, and the communications software has not been developed enough. Moreover, only a few military users can operate these freely. As a result, computer operations are being performed very inefficiently.

C. PROBLEMS AND REQUIREMENTS

In addition to the problems listed above, other factors complicate the ROKM communications situations. These include the following.

- In contrast to the tactical communications system, the strategic data communications system has not been developed.
- Although the communications equipment is well-developed, the overall communications system has not kept pace.
- In time of need, the current communications system cannot handle the demand quickly and efficiently.
- Even in peace time, the need for information exchange among each of the Armed Forces has been growing greatly.

To make things worse, the ROKM communications system must cope with technical, economic, and geographical difficulties during development, such as the following.

- In contrast to the civilian sector, the military lags behind in communications systems and communications technology.

- Military manpower for operating the systems and equipment is scarce.

- The budget is limited, but the cost of developing communications systems is very high.

- Since the ROK has a very large mountainous region (almost 70% of the land), the construction and maintenance of a communications network are very difficult.

In sum, considering all of the problems, the most serious one is that each of the Armed Forces has developed its own communications system, and there are no connections among them.

The existing communications problems of the ROKM must be considered, if a new communications network is to be successful. Thus, the design of a good data communications system model for the ROKM should meet the following requirements:

- efficiency

- cost-effectiveness

- reliability

- security

- survivability

- flexibility

These items will be developed fully in Chapter V.

III. THE UNITED STATES DEFENSE DATA NETWORK

A. HISTORY

In United States, the DDN is a large military common-user data communications internetwork. It is designed to support military operations and intelligence systems as well as general purpose automated data processing (ADP) systems and data networks having long-haul data communications requirements. The US DDN is made up of several networks. These networks have compatible hardware and software which lets them communicate with each other.

In September 1981, the Defense Communications Agency (DCA) initiated a study to assess the capabilities of the existing military Automatic Digital Network (AUTODIN II) and to evaluate a plan for an alternate system that could be used in its stead. Two separate design teams were established: (1) to develop the most survivable AUTODIN II system, and (2) to develop an alternate system based on ARPANET technology [Ref. 1].

The DCA and the Defense Science Board evaluated and compared the plans, concluding that the plan to employ ARPANET technology was more attractive to the government than the one to employ AUTODIN II technology. Thus, in April 1982, the DOD terminated the AUTODIN II program and directed that the DDN, based upon ARPANET technology, be implemented as the DOD common-user data communications network. On the basis of the DDN decision, guidance from the office of the Secretary of Defense stated:

> All DOD ADP systems and data networks requiring data communications services will be provided long-haul and area communications, interconnectivity, and the capability for interoperability by the DDN. Existing systems, systems being expanded and upgraded, and new ADP systems or data networks will become DDN subscribers [Ref. 1].

The ARPANET had been developed by the Defense Advanced Research Projects Agency (DARPA) in the 1970s. It was a purely experimental network, intended to provide efficient communications between heterogeneous computers so that hardware, software, and data resources could be shared conveniently and economically by a wide community of users. The experiment was successful, and today many data networks are modeled after the ARPANET. In September 1984, the original ARPANET was split into two separate unclassified networks. These are a military research and development network (ARPANET) and a military operational communications network (MILNET).

The DDN has evolved from its initial configuration (in 1982) to a mature configuration in four stages [Ref. 1]:

Stage I : Initial configuration was completed.

Stage II : Interfaces for terminals and additional hosts became available.

Stage III : The autonomous subnetworks were combined into a single, integrated network.

Stage IV : The network is now fully configured, with expansion continuing.

The evolution of the US DDN is depicted in Appendix A [Ref. 1].

The final configuration of the DDN is that of a multi-level secure communications network. Several operational subnetworks have been combined to form the DDN. They are:

ARPANET	Experimental Network
MILNET	Unclassified Operational Network
DISNET	Defense Integrated Secure Network
SACDIN	Strategic Air Command Digital Network
SCINET	Sensitive Compartmented Information Network
MINET	Movement Information Network (serving Europe)
WIN	Worldwide Military Command and Control System Intercomputer Network

The BLACKER technology, available in the late 1980s, will complete the DDN as a multi-level secure network.

B. OPERATIONAL USES

DDN is designed for continuous operation (24 hours a day, and seven days a week) throughout the world. The network can support at least 99% availability to any pair of "single-homed" users that want to communicate with each other. Enhanced availability will be possible by "dual-access" (two access lines to the same switching node), or by "dual-homing" (two access lines, one to each of two different switching nodes). Dual-homed users can achieve an availability of 99.95%.

The backbone network of the DDN consists of packet switching nodes (PSN). Each PSN is a Bolt Beranek and Newman (BBN) C/30-E minicomputer. They are connected together by inter-switch trunks (IST). Currently there are 174 PSNs and

300 ISTs in the backbone network. Each PSN has at least two IST circuits. A majority of the ISTs run at 56,000 bits per second (bps); some run at 9,600 bps. The network currently supports over 2,100 minicomputer and mainframe hosts.

Qualification testing is being implemented, for continuous and reliable operation of the DDN. There are two aspects of qualification testing. The first is vendor qualification of protocols (TCP/IP, etc). The second is subscriber system testing of the integration of the DOD protocols.

Appendix B contains two typical US DDN subnetwork topology maps (MILNET and ARPANET) [Ref. 1].

IV. DATA COMMUNICATIONS

A. INTRODUCTION

Data communications is the transfer of encoded information from one location to another by means of a communications channel. It involves three basic elements: (1) a sending unit (the source), (2) a transmission channel (the medium), and (3) a receiving unit (the destination). The sending and receiving units are usually computers or terminals. The transmission channel is commonly a telephone line, though data can also be transmitted in the form of radio waves, microwaves, or laser beams [Ref. 2].

Using data communications makes it possible to capture data at the point of origin. That is, data can be entered directly into the system at their source instead of being sent to some distant location for data entry and processing. A data communications network provides immediate access to information when it is needed. The advantages of using a data communications network are summarized in Table I [Ref. 2].

In this chapter, the basic concepts of data communications will be discussed, as needed for the construction of an efficient ROKM DDN.

B. COMPONENTS

In a data communications system, a communications channel links a communications control unit to one or more devices on the network. The components can be divided into

TABLE I

ADVANTAGES OF A DATA COMMUNICATIONS NETWORK

* Data capture at the information source
* Centralize control of business data
* Rapid transmission of information
* Support of rapid expansion (into dispersed locations)
* Improved management control of business data by linking

three main types. First, the Communications Control Unit (CCU) is the device controller which controls the input and output of data from and to the various devices in the network. Second, devices are the input/output hardware systems connected to the CCU; these include a variety of terminals and printers. Third, communications lines or channels connect the CCU not only to input/output devices but also to intermediate devices that facilitate the transmission of data in electronic form--modems, multi-plexers, and concentrators.

1. Communications Control Unit

To make general-purpose central computers effective for data communications, additional hardware has been developed in the form of front end modules. These modules, the CCUs, control data transmission between the central computer and remote devices. Important CCU functions include the following [Ref. 2].

(1) Connecting up to several hundred communications lines to the central computer.

(2) Adapting the main computer to a data network by converting the transmissions from remote sites into a form that the computer can accept.

(3) Polling (or monitoring) remote devices to determine their status--ready to send a message or to receive one.

(4) Storing and holding data intended for a device that is busy or temporarily out of service.

(5) Providing data protection and accountability by maintaining a message log of all transmissions.

(6) Detecting errors in message, and either correcting them or ordering a retransmission.

(7) Adding communications control codes to outgoing transmissions and deleting them from incoming ones.

(8) Determining which devices are to receive a transmission (one, some, or all).

(9) Controlling the message-priority system (if the network has one) so that the more important transmissions are processed ahead of less important ones.

2. Input/output Devices

In data communications, the terminal used may be any one of several types of input/output devices. Teletypewriter terminals have a keyboard for input and can print hard-copy output. Video terminals have a cathode ray tube (CRT) screen for displaying input from the keyboard and output from the computer. Remote-job-entry terminals are "stations" consisting of a card reader, line printer, often some kind of storage capacity for the local user, and an operator console that has a CRT screen, all of which are connected to a control unit. Transactions terminals, such as point-of-sale terminals in retail stores, are linked to a controller or minicomputer in the transaction environment itself. Intelligent terminals have a built-in microcomputer that enables them to perform such functions as transaction editing, verification, and even data base inquiry or data processing [Ref. 2].

3. Other Devices

The modem converts a digital signal received from a CCU or terminal into an analog signal that can be transmitted over a telephone line. It also converts an analog signal received over a communications channel back into a digital signal, which is the kind that computers and terminals understand.

The communications line is a path for the transmission of a signal between two points. There are two types of arrangement of lines in a network: (1) point-to-point configurations, in which a single terminal is linked to the central computer; and (2) multi-point configurations, in which the line to the computer is shared among several terminals.

The various types of communications channels will be discussed in Section D of this Chapter.

The multiplexer enables a single communications device to carry several combined signals. It does so by converting several low-speed signals to high-speed signals and transmitting them over a high-speed line.

It is cheaper to send several signals at high speed over a single line than to send them at low speed over separate lines (or over the same line). Thus multiplexing uses channels more efficiently and reduces the per-message cost.

Concentrators serve much the same basic function as multiplexers, but they have additional capabilities. Essentially, they are intelligent multiplexers. Besides combining (or pooling) messages, they can check for errors, change message codes and formats, delete extraneous characters, and temporarily store messages or parts of messages. The ability of concentrators to pool messages makes it possible to use the full capacity of a transmission line [Ref. 2].

C. THE OPEN SYSTEMS INTERCONNECTION MODEL

The International Organization for Standardization (ISO) has worked toward standardization of network architecture. The goal was to provide specific standards of implementation for the layers and the functions of networks. The Open Systems Interconnection (OSI) model was developed by the ISO as a computer communications architecture.

The OSI model defines seven layers or levels, consecutively numbered from the physical link (layer 1) to the application layer (layer 7). Figure 4.1 shows the logical structure of the the model [Ref. 3].

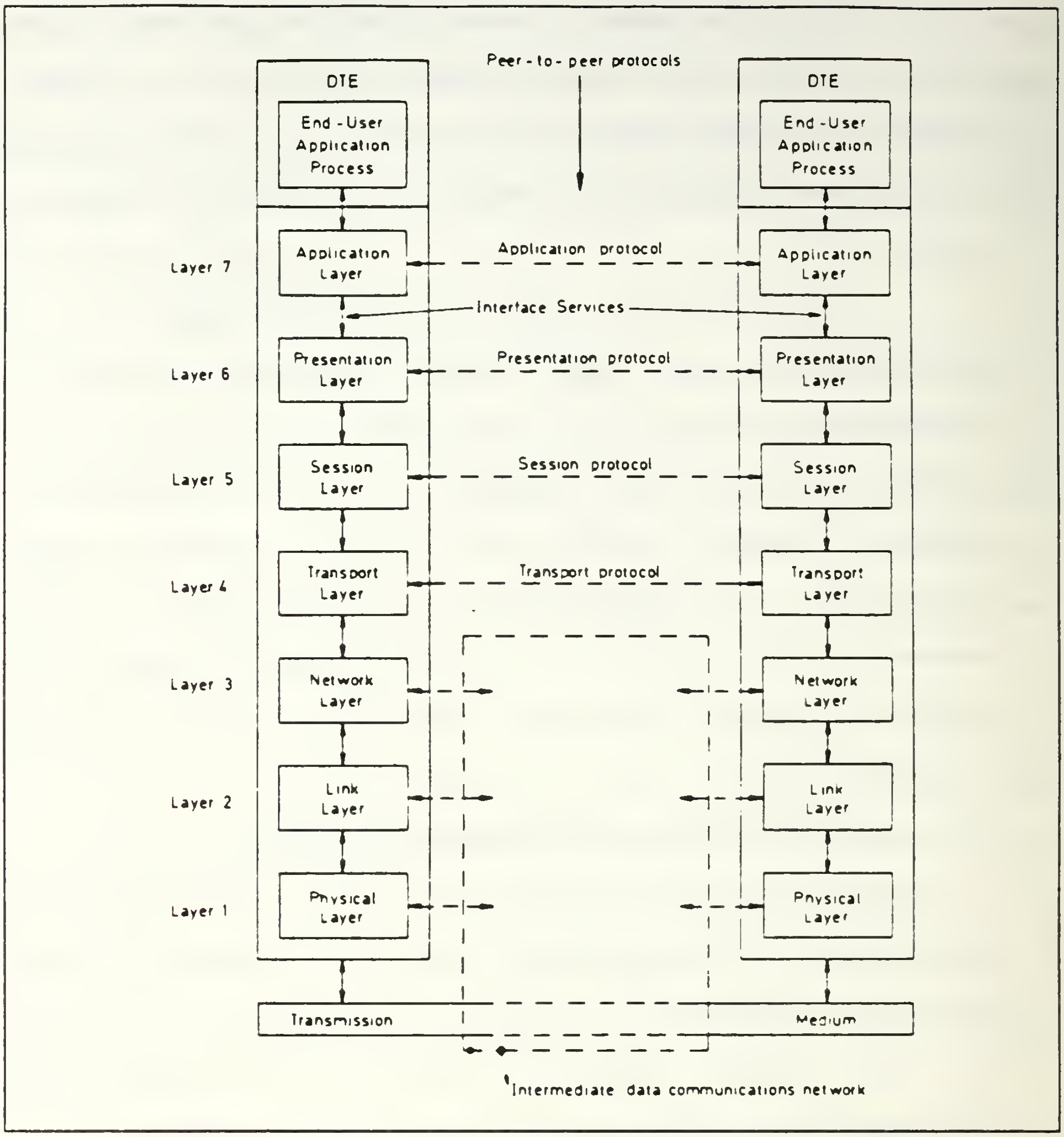


Figure 4.1 OSI Reference Model

The lowest three layers (1-3) are concerned with the communications protocols associated with the data communications network being used to link the two communicating computers together. The upper three layers (5-7) are concerned with the protocols necessary to allow the two (usually) heterogeneous operating systems to interact with each other. The intermediate layer (4) then masks the upper protocol layers from the detail workings of the lower network-dependent layers [Ref. 3]. Appendix C briefly defines the functions performed at each layer [Ref. 4].

D. TRANSMISSION MEDIA

The transmission medium is the physical path between transmitter and receiver in a data transmission system. Transmission media can be classified as hardwire (twisted pair, coaxial cable, and optical fiber cable) or softwire (air, vacuum, and seawater).

In this section, the most important hardwire media and softwire transmission techniques are discussed.

1. Twisted Pair

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. A wire pair is a single communications link, and a number of these pairs are bundled together into a cable by wrapping them in a tough protective sheath.

The twisted pair has been the most common transmission medium for both analog and digital data. It is also the medium of choice for a low-cost microcomputer local network within a building.

The twisted pair is the easiest obtainable medium and has an advantage over other media in price and cost of installation. However, compared to other transmission media, twisted pair is limited in distance, bandwidth, and data rate capability.

Figure 4.2 shows the attenuation of twisted pairs, compared with other hardwire transmission media [Ref. 4].

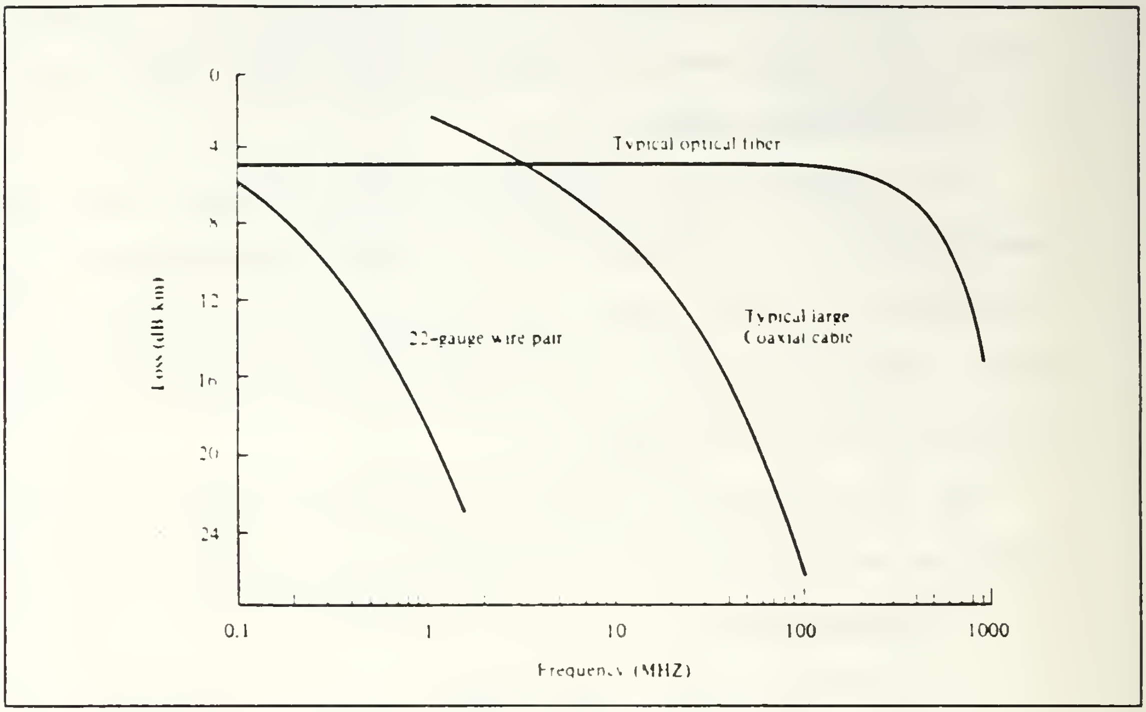


Figure 4.2 Attenuation of Typical Hardwire Media

2. Coaxial Cable

Coaxial cable consists of two conductors like the twisted pair, but it is constructed differently to permit it to operate over a wider range of frequencies.

Coaxial cable is the most versatile transmission medium. It is used in a wide variety of applications. The most important of these are long-distance telephone and television transmission, television distribution, local area networks, and short-run system links [Ref. 4].

Coaxial cable is used to transmit both analog and digital signals. Long-distance systems may be either analog or digital. Community antenna television (CATV) is an analog system, and both analog and digital techniques have been used for local networks. As seen in Figure 4.2, coaxial cable has frequency characteristics superior to those of twisted pair, and can therefore be used effectively at higher frequencies and data rates.

3. Optical Fiber

Optical fiber is a thin (50 to 100 micrometer), flexible medium capable of conducting an optical ray. Various glasses and plastics are used to make optical fibers. Fiber optic cable consists of a bundle of fibers, sometimes containing a steel core for stability.

Optical fiber is used extensively for long-distance telecommunications and military applications. The continuing improvements in performance and decline in prices (the inherent advantages of optical fiber) are expected to result in new areas of application, such as local networks and short-haul video distribution.

The following performance characteristics distinguish optical fiber from twisted pair and coaxial cable [Ref. 4].

(1) Greater bandwidth: data rates of two giga bps over tens of kilometers (km) have been demonstrated, compared with hundreds of mega bps over about one km for coaxial cable and just a few mega bps over one km for twisted pair.

(2) Smaller size and lighter weight: optical fibers are considerably smaller than coaxial cable or bundled twisted pair cable.

(3) Lower attenuation: as can be seen in Figure 4.2, attenuation is significantly lower for optical fiber than for coaxial cable or twisted pair.

(4) Electromagnetic isolation : optical fiber systems are not affected by external electromagnetic waves. Thus the system is not vulnerable to interference, impulse noise, or crosstalk.

(5) Greater repeater spacing : fewer repeaters mean lower cost and fewer sources of error.

4. Terrestrial Microwave

A microwave link usually consists of several microwave towers spaced 40 to 50 km apart. When a tower receives a signal, it amplifies the signal and retransmits it to the next tower. The most common type of microwave antenna is the parabolic "dish". The sending antenna is fixed rigidly and focuses a narrow beam to achieve line-of-sight transmission to the receiving antenna.

The primary use for terrestrial microwave systems is in long-haul telecommunications service, as an alternative to coaxial cable, for transmitting television and voice. Microwave can support high data rates over much longer distances than coaxial cable. The microwave facility requires far fewer amplifiers or repeaters than does coaxial cable for the same distance, but requires line-of-sight transmission.

A potential use for terrestrial microwave is providing digital data transmission over small regions (radius less than 10 km). This concept has been termed "local data distribution" and would provide an alternative to phone lines for digital networking [Ref. 4].

5. Satellite Microwave

A communications satellite is a micowave relay station located in a constant orbit above the earth's atmosphere. It is used to link two or more ground-based microwave transmitter/receivers, known as earth stations or ground stations.

The satellite receives transmissions on one frequency band (uplink), amplifies (analog transmission) or repeats (digital transmission) the signal, and transmits it on another frequency (downlink).

For a communications satellite to function effectively, it must remain stationary with respect to its position over the earth. To achieve this, the satellite must have a period of rotation equal to the earth's period of rotation.

Communications satellites are being used to handle telephone, telex, and television traffic over long distances. Satellite is the optimum medium for high-usage international trunks and is competitive with terrestrial microwave and coaxial cable for many long-distance international links [Ref. 4].

6. Radio

The principal difference between radio and microwave is that radio is omnidirectional, while microwave is focused. Thus radio does not require dish-shaped antennas, and the antennas need not be rigidly mounted to a precise alignment.

One use of radio for digital data communications is called packet radio, which uses ground-based antennas to link multiple sites in a data transmission network [Ref. 4].

E. MULTIPLEXING

Multiplexing is a technique of aggregating a number of low-speed signals into high-speed signals. For long-haul communications, a number of high-capacity coaxial, terrestrial microwave, and satellite microwave facilities have been built in various locations around the world. These facilities can carry large numbers of voice and data transmissions simultaneously, using multiplexing.

There are three types of multiplexing techniques. The first, frequency-division multiplexing (FDM), is the most wide spread. It is used for standard radio and television communications. The second is a particular case of time-division multiplexing (TDM) called synchronous TDM. This is commonly used for multiplexing digitized voice streams. The third type adds complexity to synchronous TDM, and is known as asynchronous TDM, statistical TDM, or intelligent TDM. Figure 4.3 shows the general case of FDM and TDM [Ref. 4].

1. Frequency-Division Multiplexing

When the useful bandwidth of the medium exceeds the required bandwidth of signals to be transmitted, FDM is possible. A number of signals can be carried simultaneously if each signal is modulated onto a different carrier frequency, and if the carrier frequencies are sufficiently

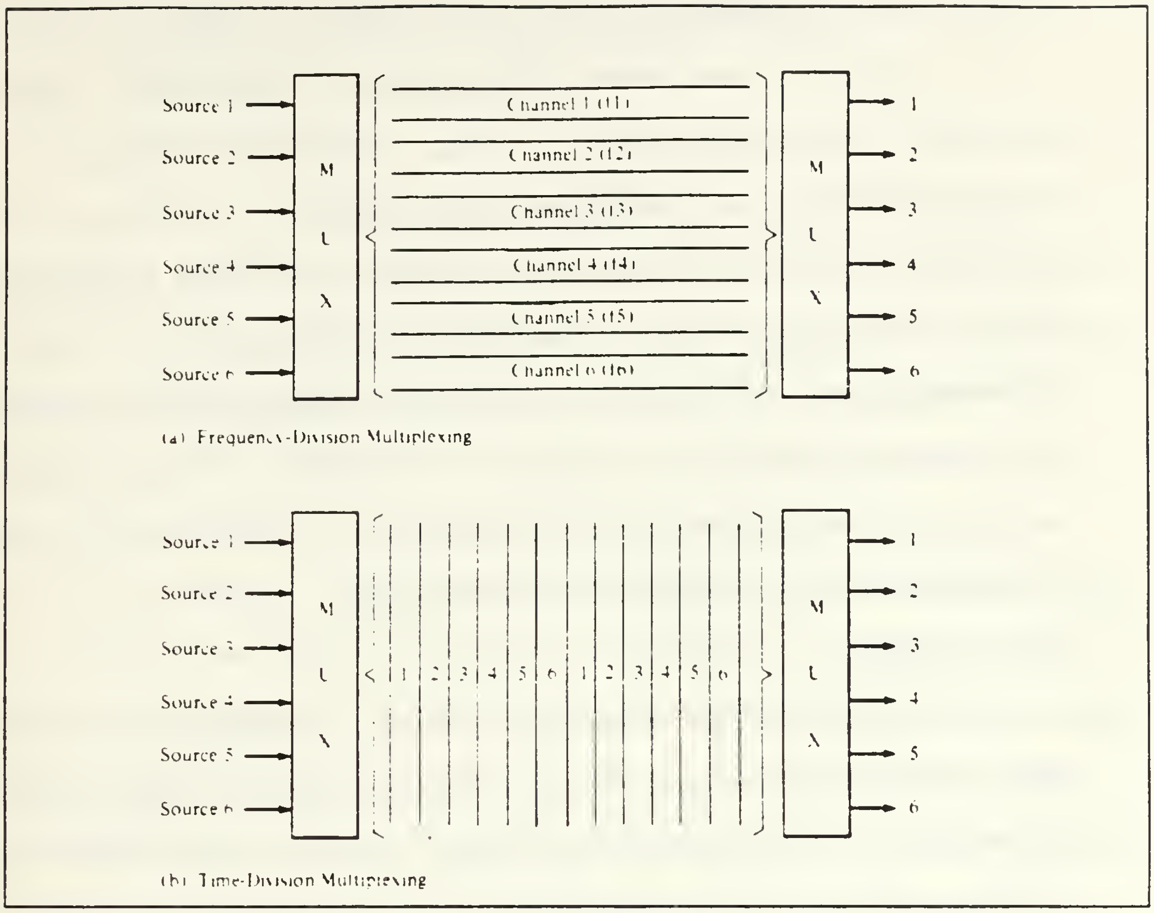


Figure 4.3 FDM and TDM

separated so that the bandwidths of the signals do not overlap.

2. Synchronous Time-Division Multiplexing

Synchronous TDM is possible when the achievable data rate (sometimes called bandwidth) of the medium exceeds the data rate of digital signals to be transmitted. Multiple digital signals or analog signals carrying digital data can be carried on a single transmission path by interleaving portions of each signal in time. The interleaving can be at the bit level or in blocks of bytes or larger quantities.

3. Asynchronous Time-Division Multiplexing

Synchronous TDM aggregates incoming low-speed channels by allocating a time slot for each, in the composite frame of the high-speed output. So the relative position of the time slot inside the frame determines to which subchannel the information belongs. In contrast, asynchronous TDM differs in that a dedicated subchannel is not provided for each terminal. Instead, a "time derived" subchannel is provided by sequential, repetitive allocation of time slots to the host channel [Ref. 5].

F. POLLING

Polling is a technique by which a shared line or a multipoint line controls the transmissions among the nodes it connects. There are two types of polling methods: roll-call polling and hub polling.

1. Roll-Call Polling

In roll-call polling, the controller or the primary station sends a message to each terminal in turn, asking whether the station needs to transmit data. Though the poll is received by all stations, each message contains the specific address of its intended terminal destination. Each station answers only its own poll. This is done by sending a "poll reject" message or the data. In the simplist case, the primary station polls each secondary station in a round-robin fashion. One problem with this method is that the overhead in polling each station can significantly increase response times if there are a large number of terminals or long communication lines between them.

2. Hub Polling

Hub polling was designed as an improvement over roll-call polling. With hub polling, the secondary station that is most remote from the primary station is polled first. If the remote secondary has data to transmit, it transmits the data to the primary, and then sends a poll to the next secondary in line. If the remote secondary has no data to transmit, it puts the address of its neighbor into the polling message. The last secondary in line sends a poll to the primary station, which then begins a new cycle. During this entire process, the primary station can be sending data to the secondary stations on the line labeled "output" in Figure 4.4, which depicts hub polling [Ref. 4].

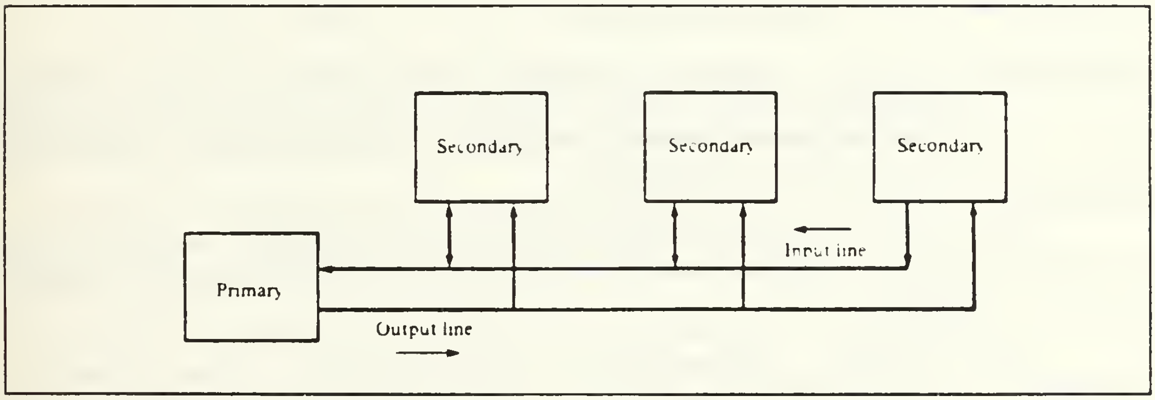


Figure 4.4 Hub Polling

G. SWITCHING

Three commonly used techniques of switching can be used to route information from one point to another. They are circuit switching, message switching, and packet switching.

1. Circuit Switching

Circuit switching is the oldest form of switching and is the method used in the public telephone network. For this form of switching, a complete transmission link path is provided from the message origination node to the destination node. A special signal message from the originating node or the interface message processor (IMP) sets up this special path. A response from the destination node then signals an acknowledgement to begin transmission to the originating node. The data is then transmitted continuously over the path with no furthur delay, and the path is dedicated to this transmission until the sender releases it [Ref. 6]. Circuit switching is depicted in Appendix D [Ref. 7].

Communications via circuit switching involves three phases, as follows [Ref. 7].

(1) Circuit establishment: creation of the dedicated physical path from source to destination; for example, a telephone number provides destination information to circuit switches.

(2) Data transfer: all information travels along the physical route that was set up during circuit establishment.

(3) Circuit disconnect: all circuits are freed upon circuit disconnect so that they can be used for other calls.

Circuit switching systems have a number of advantages, which include the following [Ref. 7].

(1) Simplest technique to implement in a switch.

(2) Most cost effective switching technique for light, intermittent loads.

(3) Least delay through the network once the circuit is established; fast enough for interactive use.

(4) Transparent to data, as no protocol or header format is required.

On the other hand, there are also disadvantages to circuit switching systems, such as the following [Ref. 7].

(1) Inefficient use of the network's available bandwidth, since the capacity of the channel is dedicated for the duration of the call.

(2) Fairly large setup delay.

2. Message Switching

Message switching was the first type of communications switching specifically tailored to the needs of computer information transfer. It is well suited to batch job processing and electronic mail applications. This type of switching is used when time is not a critical factor, since transmission delays may be significant.

This type of switching is often called store-and-forward switching. A message is stored in the first switching node and then is forwarded to the next node or IMP along its path. Each block is received in its entirety, inspected for error, and then retransmitted until it reaches the destination node. The path or route for transmission may be fixed or may be determined dynamically as the message progresses toward its destination node. Message switching is depicted in Appendix D [Ref. 7].

The advantages of message switching systems are [Ref. 7]:

(1) Line-use efficiency is much greater than with circuit switching systems, since messages from many devices will share the same node-to-node channels.

(2) Simultaneous availability of source and destination is not required.

(3) Speed and code conversion can be accomplished by the switches.

(4) Network architecture is robust, since switches can reroute subsequent messages to avoid failed network components.

(5) Message may be sent to multiple addresses simultaneously.

On the other hand, the disadvantages of message switching systems are [Ref. 7]:

(1) Messages are not switched in real time, so interactive use is not possible.

(2) Long and highly varying delays are possible.

3. Packet Switching

Packet switching attempts to combine the advantages of circuit switching with those of message switching, while minimizing the inherent disadvantages of both. Messages are transmitted a piece at a time, rather than waiting for the entire message as in message switching systems. Each piece is called a packet; packets may vary in size from implementation to implementation.

In a packet switching system, all messages are broken into standard-size packets, addressing information is attached, and packets are sent to the local packet switch for transmission to another node in the network. Packets are held in each packet switching nodes' buffers just long enough for previously-received packets to be transmitted and for error control/recovery processes to be completed. Each node forwards the packet to the next node on its route, from source node to destination node. Packet switching is depicted in Appendix D [Ref. 7].

The advantages of packet switching systems are [Ref. 7]:

(1) Packet switching provides the most efficient (cost effective) use of a network's bandwidth.

(2) Packet-switched networks are fast enough for interactive communications usage.

(3) Error free communications throughout the packet-switched network is possible, due to internal error checking and correction.

(4) Speed and code conversion are possible with packet networks.

There are also disadvantages to packet switching systems, such as the following [Ref. 7].

(1) There is slightly greater delay than with circuit-switched transmission.

(2) Unlike message switching, packet switching requires the simultaneous availability of source and destination.

Two common routing methods are used in packet switching. The simplest is fixed or static routing. Static routing is employed in virtually all public data networks since it is the easiest to implement and incurs the least network overhead traffic. In this method, all packets follow the same physical route from source to destination. The route is established at call setup time. Static routing is depicted in Appendix E [Ref. 7].

The other method is dynamic routing. Dynamic routing has been selected by the US DOD for the US DDN. With this technique, each packet may follow a different route from source to destination. The packets thus can be routed over the optimum path at any given time. Upon receipt of a packet, each packet switch determines the best path over which to route the packet next, so that it will arrive at its destination in the least amount of time, and then forwards the packet over that route. Dynamic routing thus provides the network with the ability to reconstitute itself in the event that one or many of the network components are damaged. Dynamic routing is depicted in Appendix E [Ref. 7].

Static and dynamic routing packet networks can be compared as follows [Ref. 7].

(1) Dynamic routing provides for a more robust network. Packets will reach their destinations by alternate means if a line or node suddenly fails.

(2) Error detection/correction is simpler in statically-routed systems since correct packet sequencing is inherent to the system. In a dynamically routed network, there is a possibility of packets arriving out of order. The re-assembly process is complicated by the fact that the receiver does not know if a packet is missing or just delayed.

(3) The possibility of oscillation (a packet being routed over the same paths over and over again) exists in a dynamically-routed network.

(4) Dynamically-routed systems will provide faster transmission, since each packet will be routed over the quickest path at any given time. Statically-routed packets must traverse the same route for the entire duration of the call.

V. SYSTEM ANALYSIS

A. INTRODUCTION

Current ROKM communications problems and requirements have been enumerated in Chapter II. The US DDN and the basic concepts of data communications have been covered in Chapter III and IV, with emphasis on how these apply to the construction of an efficient ROKM DDN. The purpose of this chapter is to discuss more specific issues that may play an important role in designing a ROKM DDN.

The first section of this chapter describes the objectives of the proposed system. The second part further develops the current ROKM communications requirements (the goals of new network) which were introduced in Chapter II.

B. ROKM DDN OBJECTIVES

The major mission of the ROKM is to defend its country from the invasion of North Korea or neighboring communist countries. To achieve this important mission, the ROKM must maintain the best possible defense capability and continuously improve combat readiness.

The first objective of ROKM DDN is to improve combat readiness capability. Via this system, urgent and important messages can be exchanged rapidly among all of the Armed Forces. This will contribute to good decision making and to interservice cooperation regarding sharing of information, joint operations, and supply cooperation. In addition, the system can be used as a general-purpose data and information exchange network and as an experimental, or research network.

Office automation is another objective of the ROKM DDN. The application of computer and communications technology will improve the productivity of clerical and managerial office work.

C. ROKM DDN GOALS

Goals of the ROKM DDN should be based on unmet needs and on the characteristics of current kinds of work that will be performed using the new network. Using this approach, several desirable goals can be identified.

1. Efficiency

This refers to effective resource sharing, beginning with data that will be commonly shared among all stations. Efficiency can be enhanced by easy user access to all workstations. The common use of printers and other computer peripherals is another aspect of resource sharing.

The speed at which data can be accessed is another consideration. The higher the speed, the more effective the network. In addition, the system must be well-organized in order for the user to understand and operate it easily and efficiently.

2. Cost-effectiveness

Considering the economic constraints of the military organization, this is probably the most critical factor. A good ROKM DDN must balance the need for a reliable, efficient system against the cost of such a system.

3. Reliability

Reliability is the probability that a system or component will perform its specified function under specified conditions [Ref. 8]. High system reliability is essential to the military network. To achieve this, an error detection and an error correction mechanism must be built into the network to reduce the number of possible errors.

4. Security

Security is the protection of network resources against unauthorized disclosure, modification, utilization, restriction, or destruction [Ref. 8]. Because of this network's military application, levels of security should be built into the network. The ROKM's recognized sensitivity levels, in order of impact on the national security, are:

* Classified

  - Top secret (I)
  - Secret (II)
  - Confidential (III)

* Unclassified

Security is critical for a military network. If sensitive communications were intercepted by the enemy, it could be potentially damaging to the national defense.

5. Survivability

Survivability is critical to any military network, but especially so for the ROKM DDN. Since the Korean peninsula is small and North Korea's main attacking forces are posted very close to the ROK, sudden attack by North Korea is possible. Continuity of the network's operation under conditions of attack is an important factor for the proposed network system.

6. Flexibility

The ROKM DDN should interface with existing computer and communications facilities. It should also have the versatility to expand, at minimal cost, as necessary for the growth of each of the departments of the military.

VI. PROPOSED MODEL

A. INTRODUCTION

This chapter develops a specific model that may be used for designing a data communications network for the ROKM. Data communications network issues are carefully examined in order to provide the required levels of data communications capabilities and network performance.

The first two sections of this chapter discuss the network structure and software needed in the design of the ROKM DDN. The following three sections develop other important considerations--performance, security, and survivability. Throughout this chapter, current technology of the US DDN is applied to the model.

B. ROKM DDN STRUCTURE

A computer-communications network is an interconnection of several computers, or a set of terminals connected to one or more computers [Ref. 9]. Figure 6.1 represents a typical computer communications network structure (US DDN) [Ref. 1]. This is the proposed ROKM DDN model.

Host mainframes can be directly connected to DDN backbone, which is composed of PSNs. This requires that all subscriber hosts make use of the required DDN protocols. Host implementation can provide full DDN networking services such as establishing host-to-host, terminal-to-host, and host-to-terminal connections. On the other hand, connections

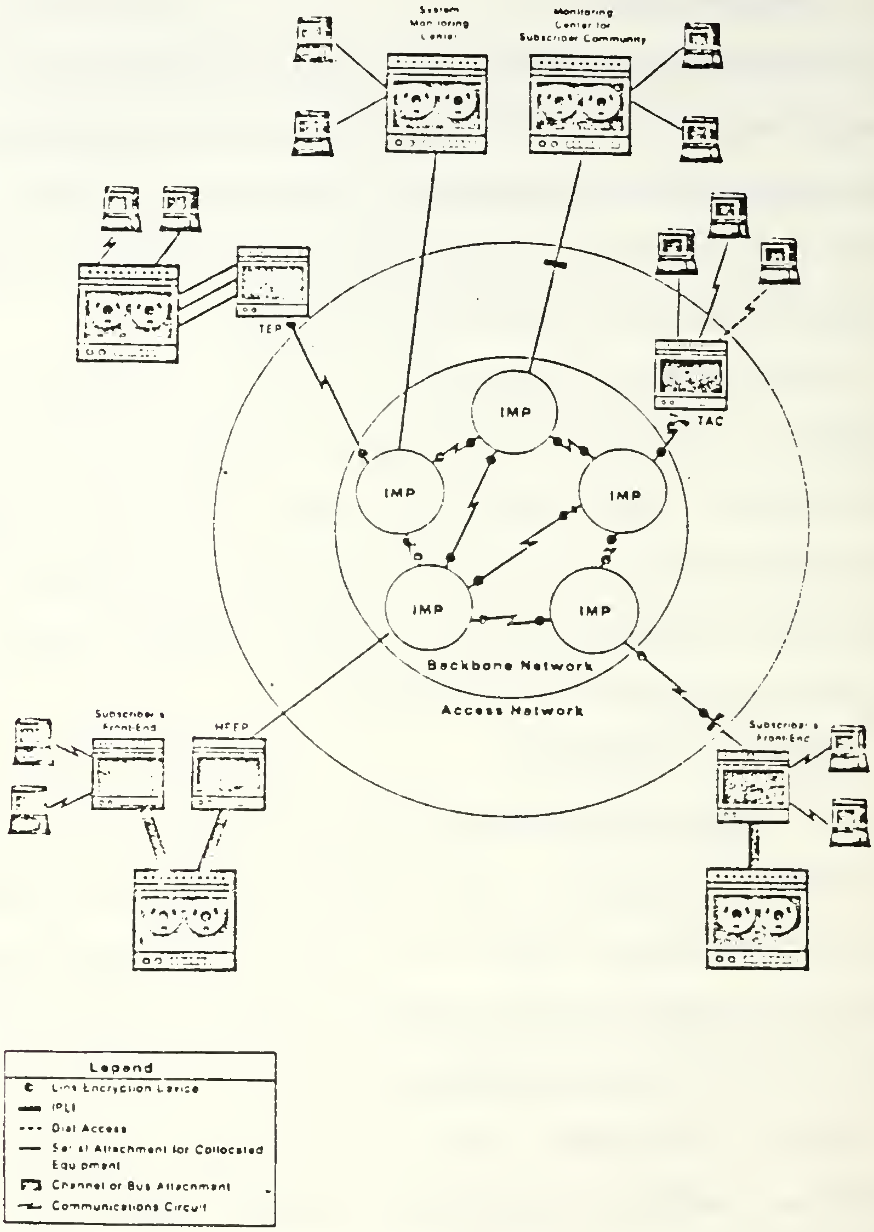


Figure 6.1 Structure of Computer Communications Network Proposed as a Model for the ROKM DDN

between terminals and hosts may be constrained by access controls and terminal type differences [Ref. 10].

Another method to achieve host access is through the use of a front-end processor. In this method, host protocols are implemented in the host front-end processor (HFEP) which in turn communicates with the host by a simpler host front-end protocol. The HFEP contains all of the required protocols to allow for full DDN networking services and connections to the backbone [Ref. 10].

In addition, there is one more method by which a user host may access the DDN. The device called a terminal emulation processor (TEP) can link a host to a backbone PSN. In this method, host protocols are implemented in the TEP which is connected to terminal ports on the host. Since the TEP emulates terminals, a host connected to the network using this approach can regard the network only as a set of locally attached terminals. Therefore, full networking services are unavailable and the TEP is not recommended [Ref. 10].

Individual terminals can access the DDN in two ways: (1) via a subscriber host, and (2) using a terminal access controller (TAC). Connection to a TAC may be established via serial attachment for collocated equipment, via a communications circuit, or by telephone dial-in.

The network monitoring centers (NMC) complete the DDN network structure. NMCs check the status, topology, and throughput of the network. It is also possible for a subscriber community to establish its own monitoring capability.

Appendix F depicts three DDN access devices [Ref. 7].

C. SOFTWARE

Protocol is a set of conventions or rules that allows two end points to communicate [Ref. 11]. The DDN must enable interoperation of numerous makes of computers, terminals, and independent networks for various organizations. Therefore, the DDN requires that the hosts have suitable software, implementing the required protocols [Ref. 1]:

(1) Transmission Control Protocol/Internet Protocol (TCP/IP), protocols that permit the end-to-end flow of data between two computer systems or between a host system and a TAC.

(2) File Transfer Protocol (FTP), a protocol that enables files to be transferred between computer systems.

(3) Telnet (TN), a virtual terminal protocol, to which traffic from different terminal types is converted, resulting in the use of a common virtual terminal format throughout the network.

(4) Simple Mail Transfer Protocol (SMTP), a protocol used to transfer mail reliably and efficiently.

(5) Gateway Protocols, protocols that enable communications between several independent networks.

In addition, to be interoperable, subscriber systems must conform not only to these protocols but must also possess application programs which make use of these protocols [Ref. 1].

1. TCP and IP

TCP provides reliable host-to-host transmission. Reliability results from (1) the use of positive acknowledgement to guard against lost segments, (2) checksumming to protect against damaged segments, (3) sequence numbering to protect against duplicate or out-of-order segments, and (4) flow control to guard against network congestion [Ref. 12].

TCP provides numerous services, such as:

(1) Data Transfer: allows users to send or receive a continuous stream of data and prepares packets for transmission [Ref. 13].

(2) Reliability: provides for end-to-end acknowledgement of packets and the retransmission of unreceived packets [Ref. 14].

(3) Flow Control: allows the receiver to control the amount of data transmitted using window protocol (which indicates the allowed number of bytes that the sender may transmit) [Ref. 7].

(4) Multiplexing: provides a set of addresses or ports for each host to allow many processes within a host to use TCP simultaneously [Ref. 7].

(5) Connections: provides for a logical connection.

(6) Precedence: user may indicate the priority of the transmission.

IP supports data transmission across multiple packet switched networks. IP is potentially unreliable and depends upon TCP or other protocols to guard against lost or damaged data. The basic function is to fragment packets for entry into "small packet" networks and for reassembly of fragmented packets at the destination [Ref. 12].

Once access to the DDN backbone is achieved, the IP controls packet switching through the subnetwork. For this service, the physical addresses of source and destination are needed.

TCP and IP are closely related with each other in the protocol layering implementation process [Ref. 13].

2. FTP

FTP allows file transfer from one host to another and provides access to file manipulation functions. To make this possible, a set of conventions has been agreed upon for file structure and DDN users will be required to utilize file formats that make use of this protocol [Ref. 1].

FTP implementations are integrated with a host's file management system to provide the following common network capabilities [Ref. 15]:

(1) access to both source and destination file management systems--in effect, simultaneous log-ins;

(2) transformation between source and destination file formats;

(3) ability to direct the transfer of large volumes of data in the presence of potential network failures;

(4) other file manipulation functions such as directory listings, appending, deleting, etc.

3. TN

TN provides for terminals attached to hosts or TACs to communicate with remote hosts. The network virtual terminal (NVT) mechanism provides this communications. The NVT maps the terminal characteristics into a network standard. At the remote host end of the connection, the network standard is mapped into a set of terminal characteristics that is recognized by that host, thus creating the illusion that the remotely located terminal is a locally attached terminal [Ref. 16].

FTP commands are transferred via TN; therefore, the TN protocol must be implemented in all hosts for FTP to be utilized [Ref. 17].

4. SMTP

SMTP supports efficient and reliable transfer of electronic mail over the DDN. Mail transmission protocols include standard formats for the following items [Ref. 7]:

(1) Destination host and mailbox name.

(2) Reverse-path, recording whom the mail is from (return route).

(3) Forward-path, recording whom the mail is sent to (source route).

If a server-SMTP cannot deliver mail for any reason, it must create an "undeliverable mail" message and send it to the originator of the undeliverable mail [Ref. 7].

5. Gateway Protocols

Gateway protocols are used to connect other networks to the DDN. As more gateways are added, the complexity and buffering requirements are beyond the capabilities of the hardware and software. Therefore, homogeneous gateways under a single authority and control are best for maintainability and operability [Ref. 7].

There are two kinds of gateway protocols, as follows [Ref. 7]:

(1) Gateway-Gateway Protocol (GGP): used with IP to determine connectivity to networks and neighbor gateways.

(2) Exterior Gateway Protocol (EGP): conveys network reachability information between neighboring gateways.

D. PERFORMANCE

The DDN should be designed to satisfy the performance needs of computer system users who require data communications services. The ROKM network equipment should be designed to minimize delay, detect and correct errors, ensure proper delivery of messages, and maximize the availability of network services.

To make the DDN efficient, the following requirements should be met [Ref. 1].

(1) The network effectively serves interactive users.

(2) Data are transmitted accurately and fast.

(3) Data packets are delivered to their intended destinations.

(4) Services are available when required.

Table II presents a summary of US DDN projected performance [Ref. 1]. This can serve as a guideline for the ROKM DDN performance.

E. SECURITY

The ROKM DDN should provide services for its users that comply with DOD security policy, through cryptographic separation of user communities, protection from unauthorized denial of service, protection from unauthorized analysis of traffic flow, and protection from the compromise of sensitive information [Ref. 1].

The ROKM DDN should incorporate safeguards that are presently used in the US DDN, as follows [Ref. 1]:

TABLE II

PROJECTED PERFORMANCE OF US DDN

AVAILABILITY	
For Single-homed Subscribers	99.30%
For Dual-homed Subscribers	99.99%
END-TO-END DELAY	
Average:	
For High-Precedence Traffic	0.090 Seconds
For Routine-Precedence Traffic	0.122 Seconds
Ninety-Ninth Percentile	
For High-Precedence Traffic	0.224 Seconds
For Routine-Precedence Traffic	0.458 Seconds
PROBABILITY OF UNDETECTED ERROR	$4.2\text{x}10^{-18}$
PROBABILITY OF MISDELIVERING PACKET	$5.5\text{x}10^{-12}$

(1) link encryption

(2) end-to-end encryption

(3) physical security at sites with packet switches

(4) use of cryptographic authentication protocol

(5) use of only TEMPEST-approved equipment

Link encryption should be used on all ROKM DDN network backbone links, all access lines to classified hosts and TACs, and on access lines to all monitoring centers. End-to-end encryption should be provided by internet private line interface (IPLI) to safeguard classified information transmitted through the network. A cryptographic authentication protocol should be used for all traffic between monitoring centers and packet switches to prevent unauthorized transmission of switch-control messages. Packet switches should be placed in areas that are approved for handling and storing data that is classified at least at the secret level. Network elements should be TEMPEST-approved to ensure that their electromagnetic eminants are minimized, and thus are protected from unauthorized analysis [Ref. 1].

Figure 6.2 summarizes all proposed safeguards for the ROKM DDN, needed to support security and privacy [Ref. 1].

F. SUVIVABILITY

The ROKM DDN should be a highly distributed network in order to survive possible damage. The following network features should enable the DDN to continue providing service to subscribers even when it is partially damaged [Refs. 1, 7]:

(1) Much of the network equipment should be in facilities at least as survivable as the facilities of the subscribers that rely upon the equipment.

(2) Critical equipment and circuits should be configured redundantly.

(3) If the network is damaged, the quality of service should degrade gracefully; the network will respond automatically to such failures by routing traffic around all inoperative components.

(4) Switching nodes should be widely dispersed over the system and whenever possible located away from targeted areas.

(5) Dynamic adaptive routing automatically should route traffic around congested, damaged, or destroyed switches and trunk circuits, allowing the system to continue working over the remaining portions of the network.

(6) DDN should provide precedence and preemption capabilities to ensure that critical, time sensitive data can get through in the event of surges in traffic during peace-time, or in the event of degraded network capabilities due to stress conditions.

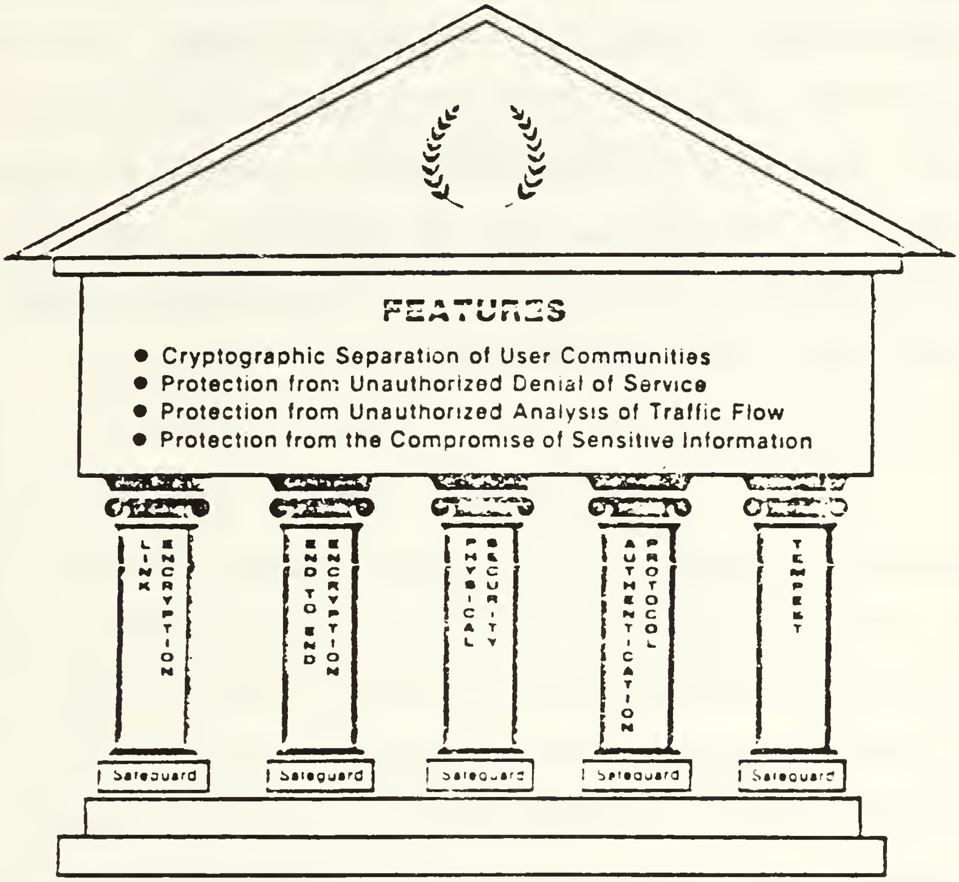

FEATURES
● Cryptographic Separation of User Communities
● Protection from Unauthorized Denial of Service
● Protection from Unauthorized Analysis of Traffic Flow
● Protection from the Compromise of Sensitive Information
LINK ENCRYPTION
END TO END ENCRYPTION
PHYSICAL SECURITY
AUTHENTICATION PROTOCOL
TEMPEST
Safeguard
Safeguard
Safeguard
Safeguard
Safeguard

Figure 6.2 Safeguards to Support Security and Privacy for the ROKM DDN

(7) To facilitate system reconstitution in the event of extreme stress or post-attack, several mobile reconstitution nodes, equipped with NMC capability, should be positioned in the least targetable areas.

To protect the network's transmission base further, the ROKM DDN should incorporate a diversified set of transmission services. These include a variety of terrestrial, radio based, and satellite capabilities, provided by both military and multiple commercial carriers. This diversity of transmission media reduces the network's vulnerability to carrier problems, acts of sabotage, jamming and other electronic countermeasure (ECM) attacks, and to other threats to the transmission base [Ref. 18].

VII. CONCLUSIONS

A. SUMMARY

Because of Korean geography and political environment, the ROK presently has large armed forces, and may require even stronger Armed Forces in the future for national defense. An adequate communications system plays a critical role in national defense, and the importance of computer communications systems is growing greatly. The ROKM presently has conventional communications networks for each of the Armed Forces individually, but has no data communications network. Therefore, an integrated computer communications network is needed urgently by the ROKM, for efficient communications and national defense.

This thesis has provided the key concepts for designing a computer communications network for the ROKM. In the first part of this study, the current ROKM communications system and its problems and requirements were discussed. Next, the basic concepts of data communications and current aspects of US DDN were introduced. In the last part of this study, the system's goals were fully developed and a proposed ROKM DDN model was provided for the construction of an efficient ROKM DDN.

B. RECOMMENDATIONS

When developed, the ROKM integrated computer communications network should be designed to meet the ROKM DDN goals which were developed in Chapter V. Moreover, because of its military uses, the ROKM DDN must be designed and implemented circumspectly, that is, with careful consideration of all circumstances and possible consequences. For implementation of a successful integrated computer communications network for the ROKM, It is strongly recommended that the following basic elements be considered during development:

(1) Numerous brands of computers can be used for PSNs, TACs, NMCs, gateways, hosts, and terminals. The ROKM should use standard computers which offer the best performance at the lowest price.

(2) The ROKM currently uses many communications links. The ROKM DDN may continue to use these links, but a dedicated data communications channel also is needed, like the US DDN.

(3) The ROKM DDN will need many kinds of software for the network backbone, gateway computers, and host computers to communicate throughout the DDN and provide DDN access for users. Standard software should be developed or obtained, for compatibility (including compatibility with the US DDN).

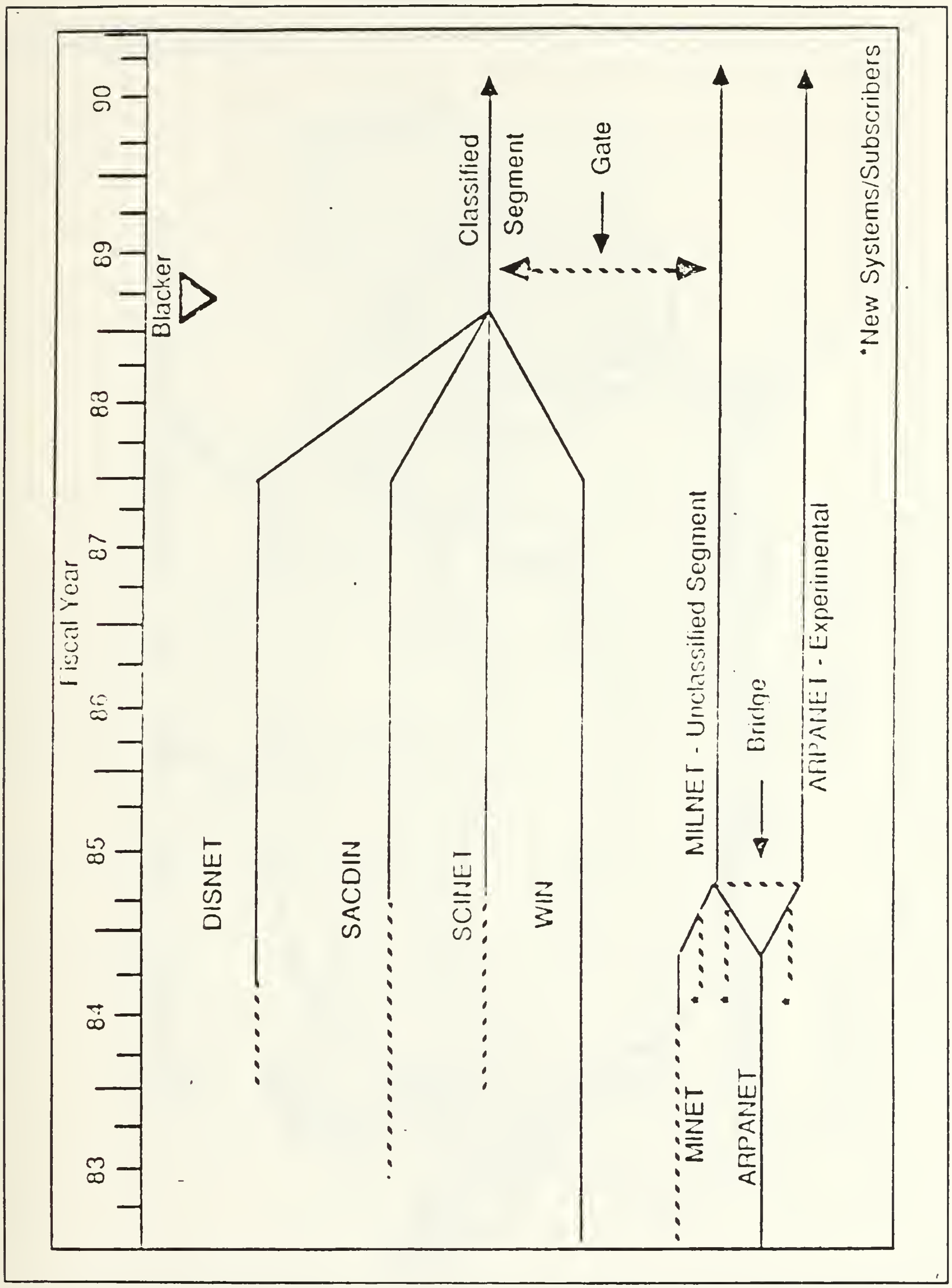
(4) Network security and survivability must be a primary consideration, throughout ROKM DDN development.

Because of lack of actual data about the ROKM, this paper has just provided the general concepts for building a ROKM DDN. In the near future, these concepts should be developed further and detailed installation and implementation plans should be prepared.

It is expected that this study can serve as a guideline or partial solution for constructing a computer communications network that is needed to connect all of the ROK Armed Forces.

APPENDIX A

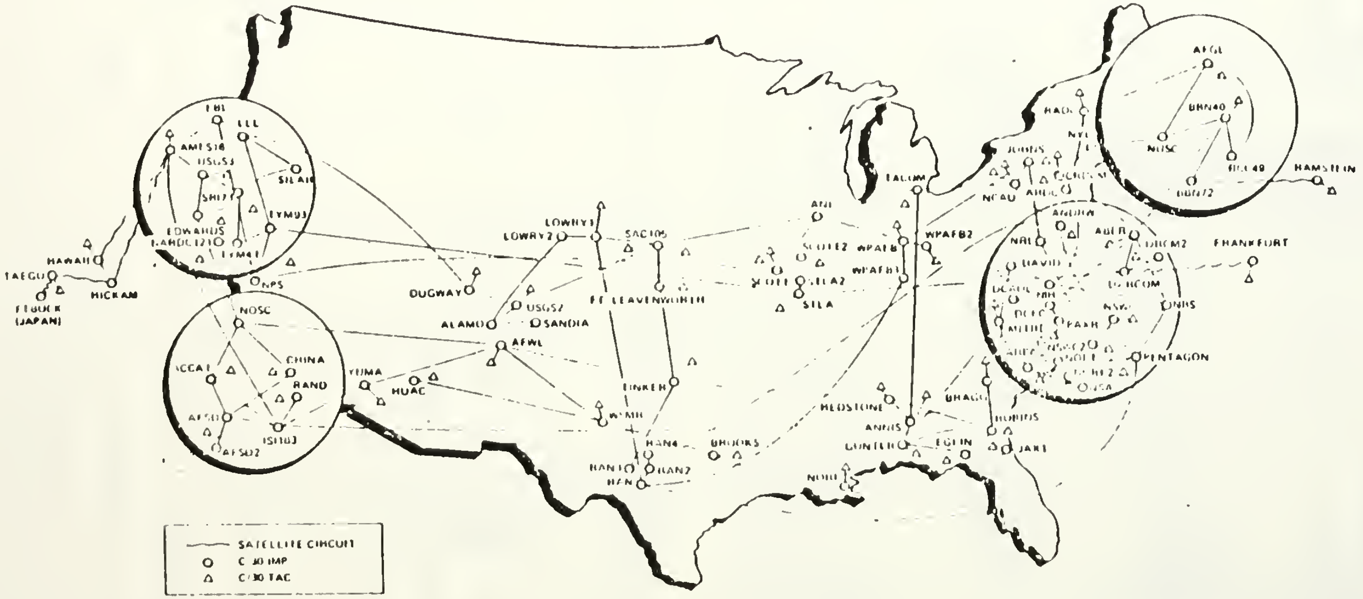
US DDN SCHEDULE



APPENDIX B

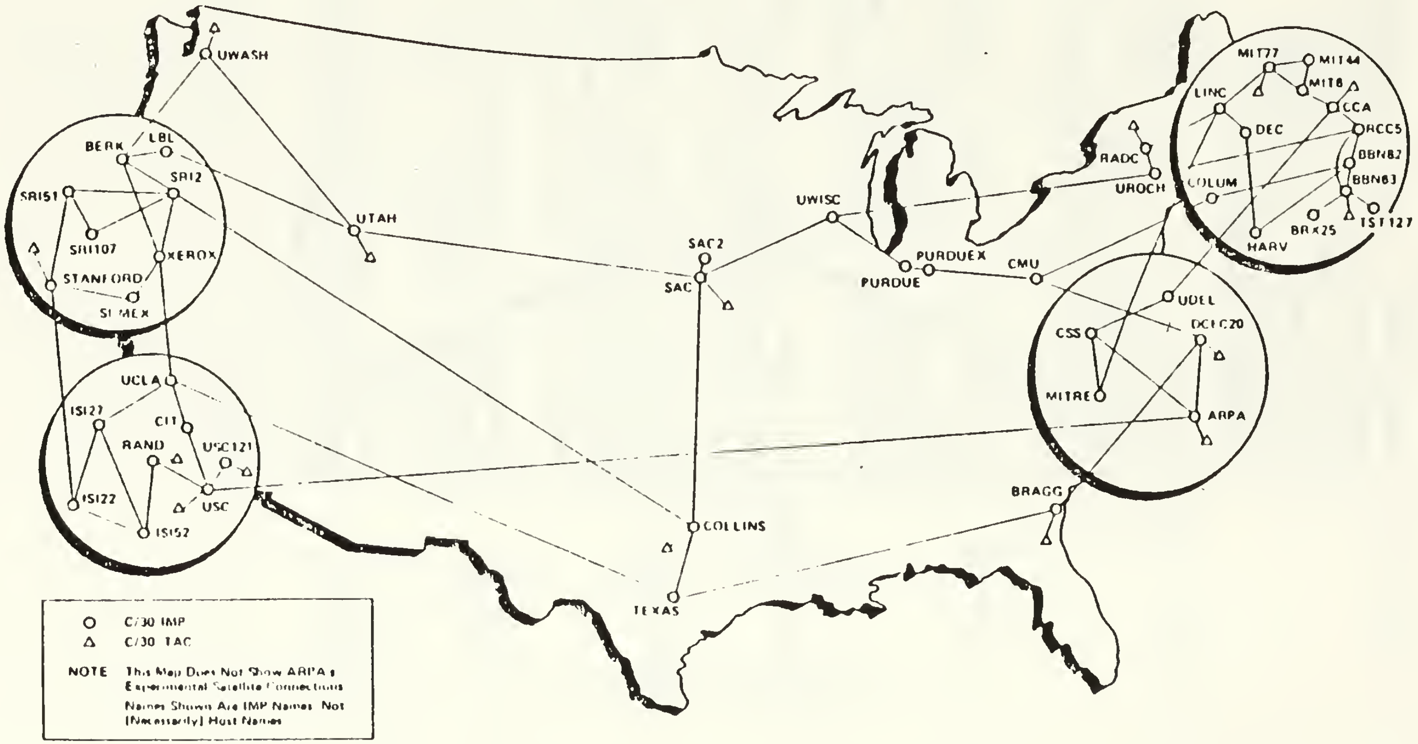
US MILNET

MILNET Geographic Map, 30 September 1985



US ARPANET

ARPANET Geographic Map, 30 September 1985



○	C/30 IMP
△	C/30 TAC

NOTE This Map Does Not Show ARPA's Experimental Satellite Connections

Names Shown Are IMP Names, Not (Necessarily) Host Names

APPENDIX C

THE OSI LAYERS

1. Physical Concerned with transmission of the unstructured bit stream over physical medium; deals with the mechanical, electrical, functional, and procedural characteristics related to accessing the physical medium.

2. Data Link Provides for the reliable transfer of information across the physical links; sends blocks of data (frames) with the necessary synchronization, error control, and flow control.

3. Network Provides the upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining and terminating connections.

4. Transport Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control.

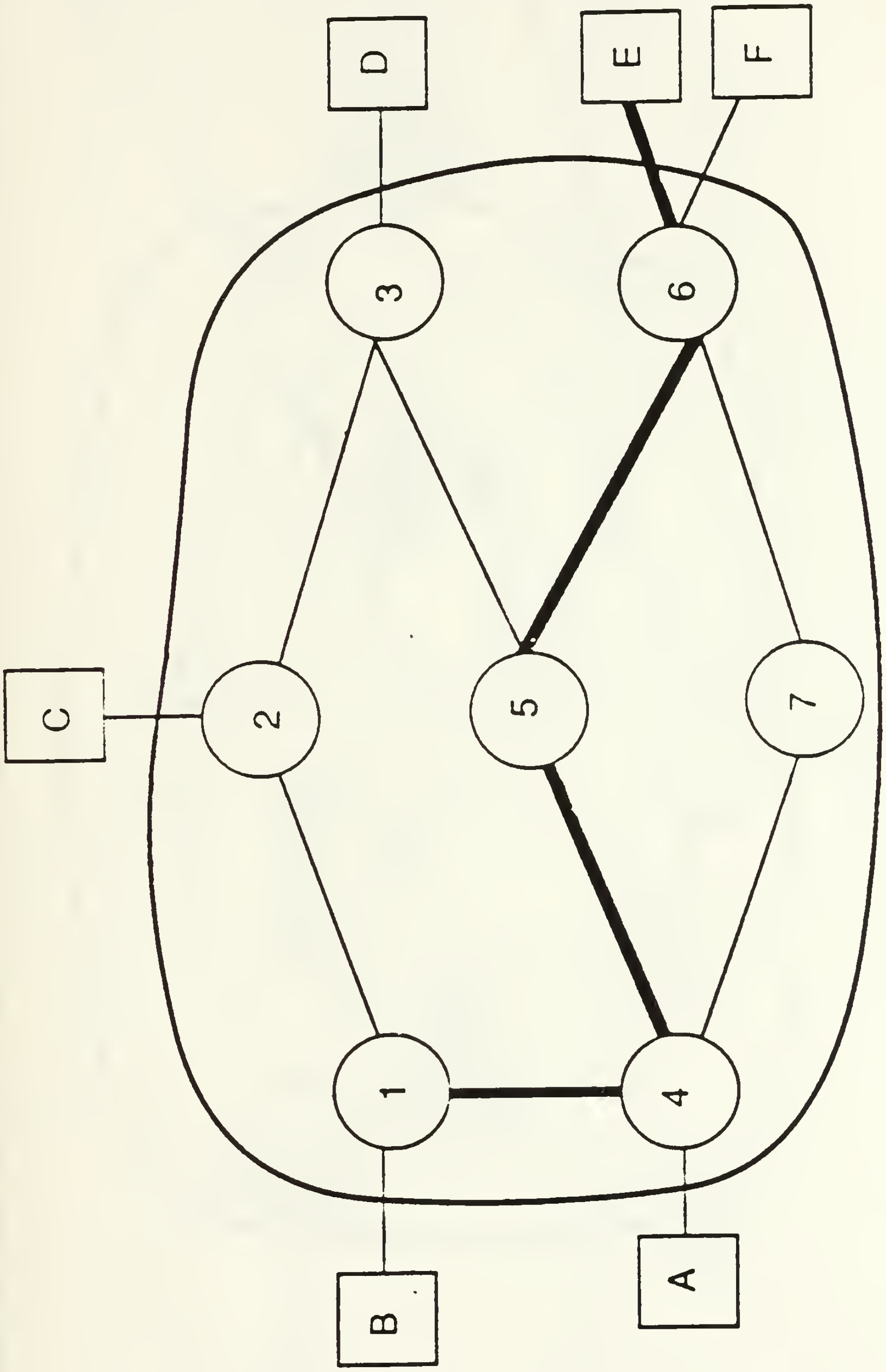
5. Session Provides the control structure for communication between applications; establishes, manages,and terminates connections between cooperating applications.

6. Presentation Provides independence to the application processes from differences in data representation (syntax).

7. Application Provides access to the OSI environment for users and also provides distributed information services.

APPENDIX D

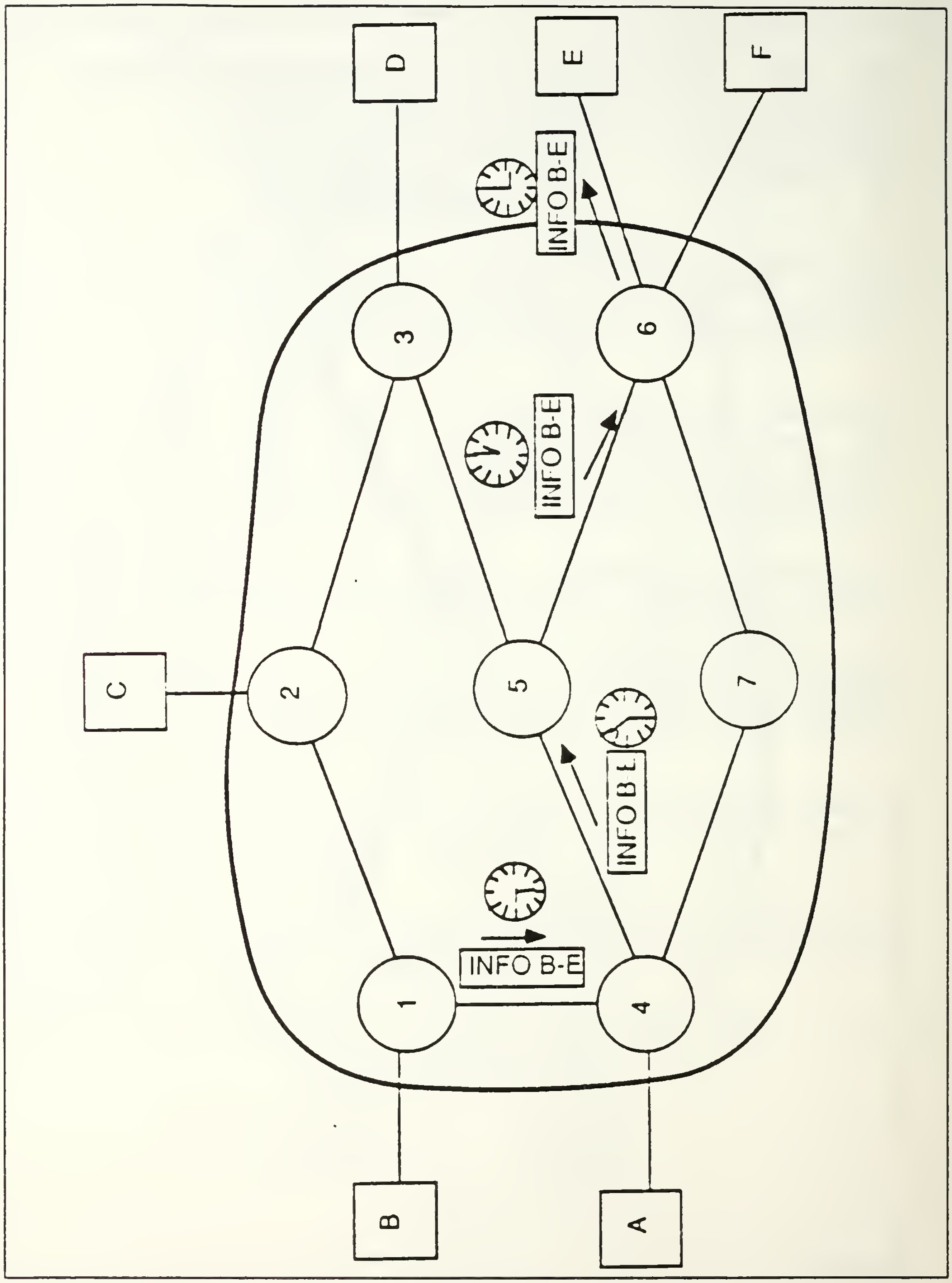
CIRCUIT SWITCHING



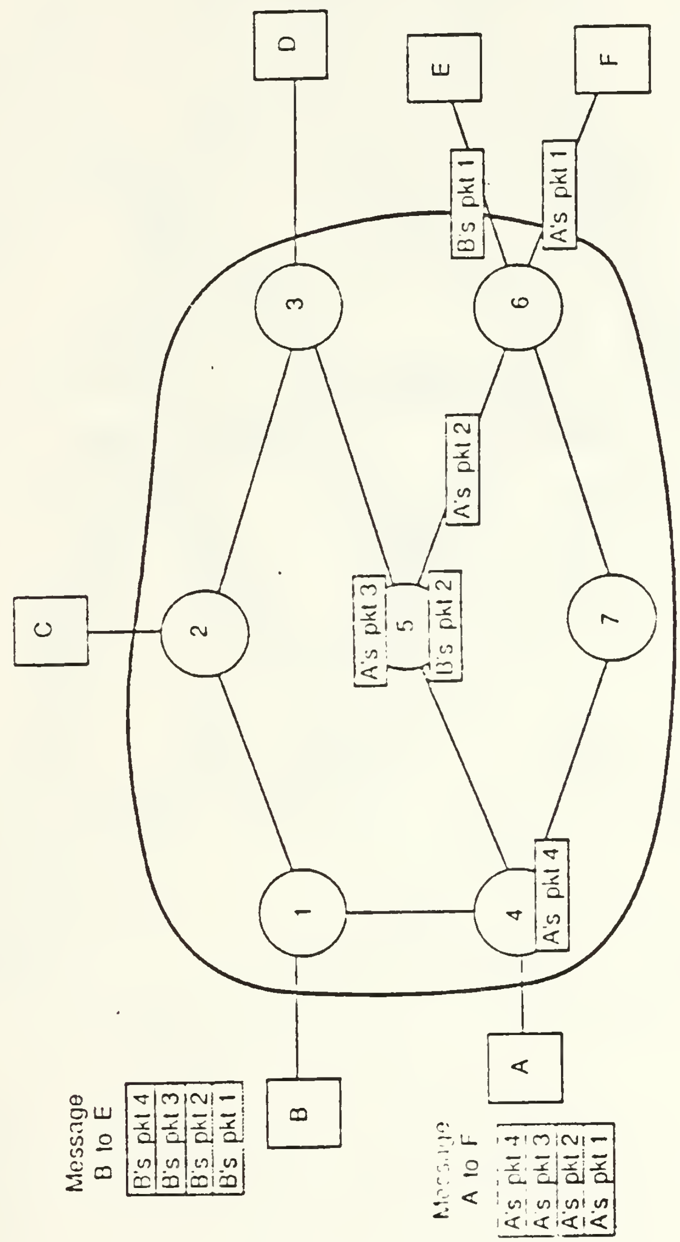
Call Connecting B to E

Note that A cannot call B, C, D or E until call is terminated

MESSAGE SWITCHING

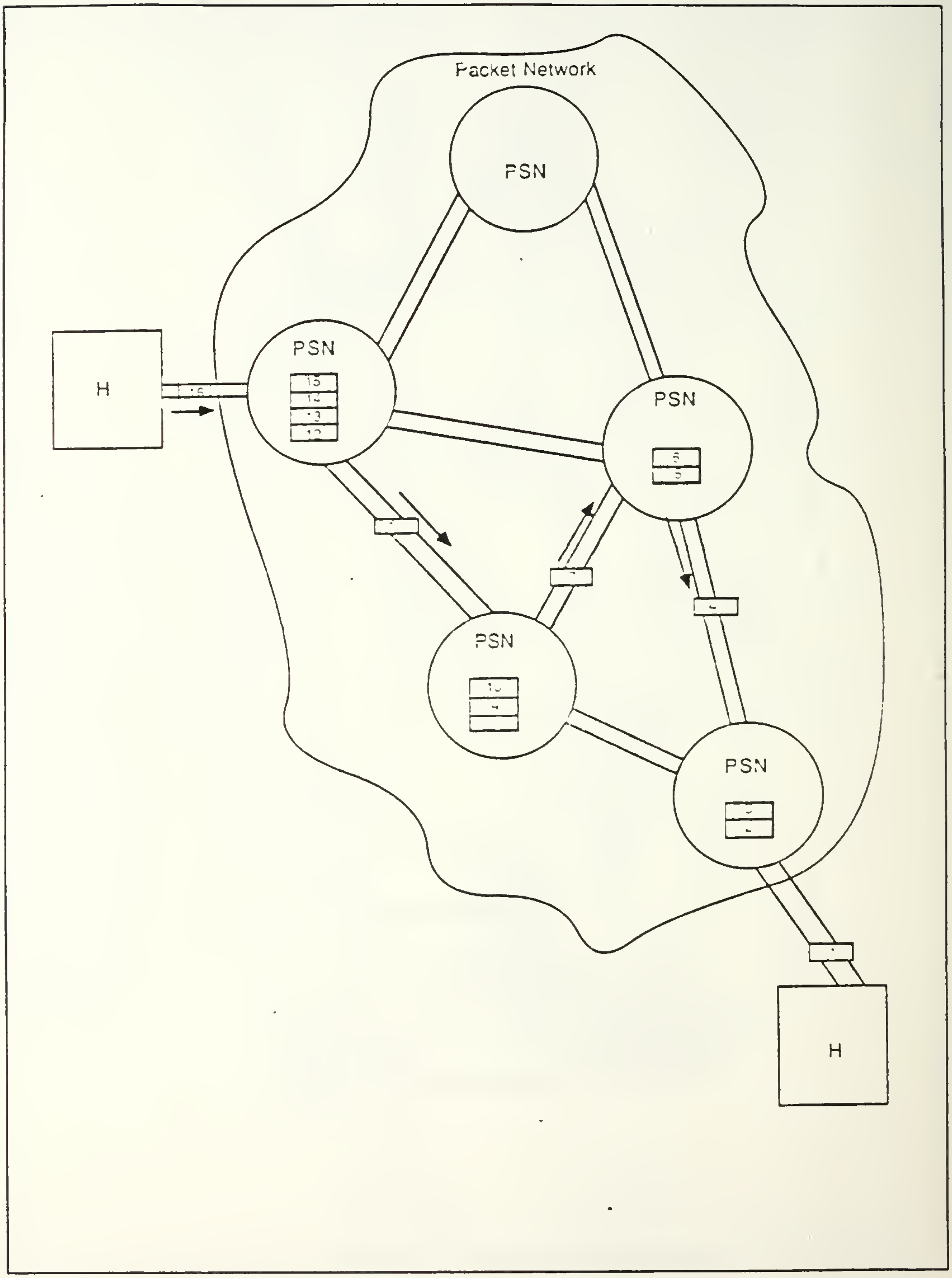


PACKET SWITCHING

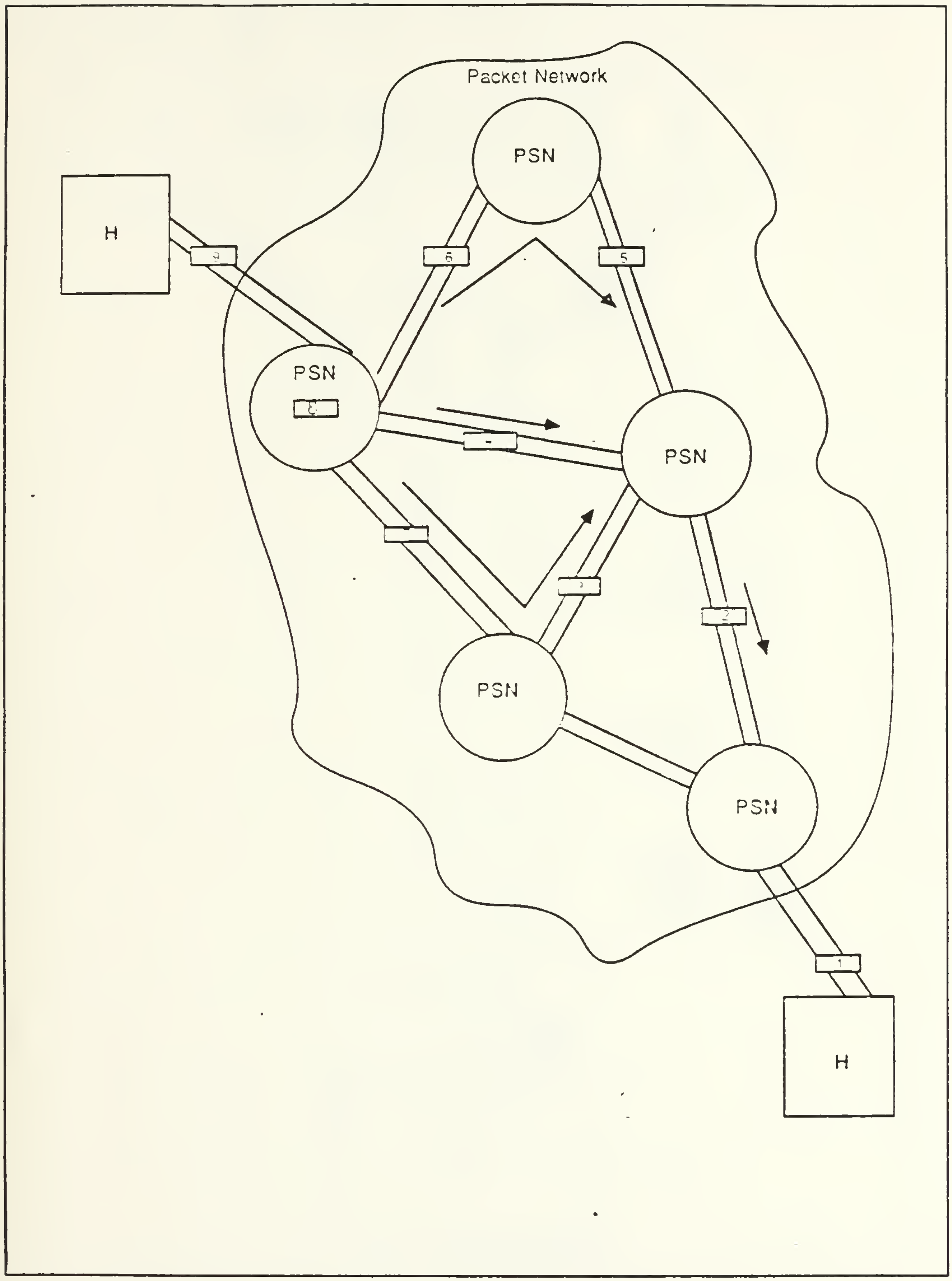


APPENDIX E

STATIC ROUTING

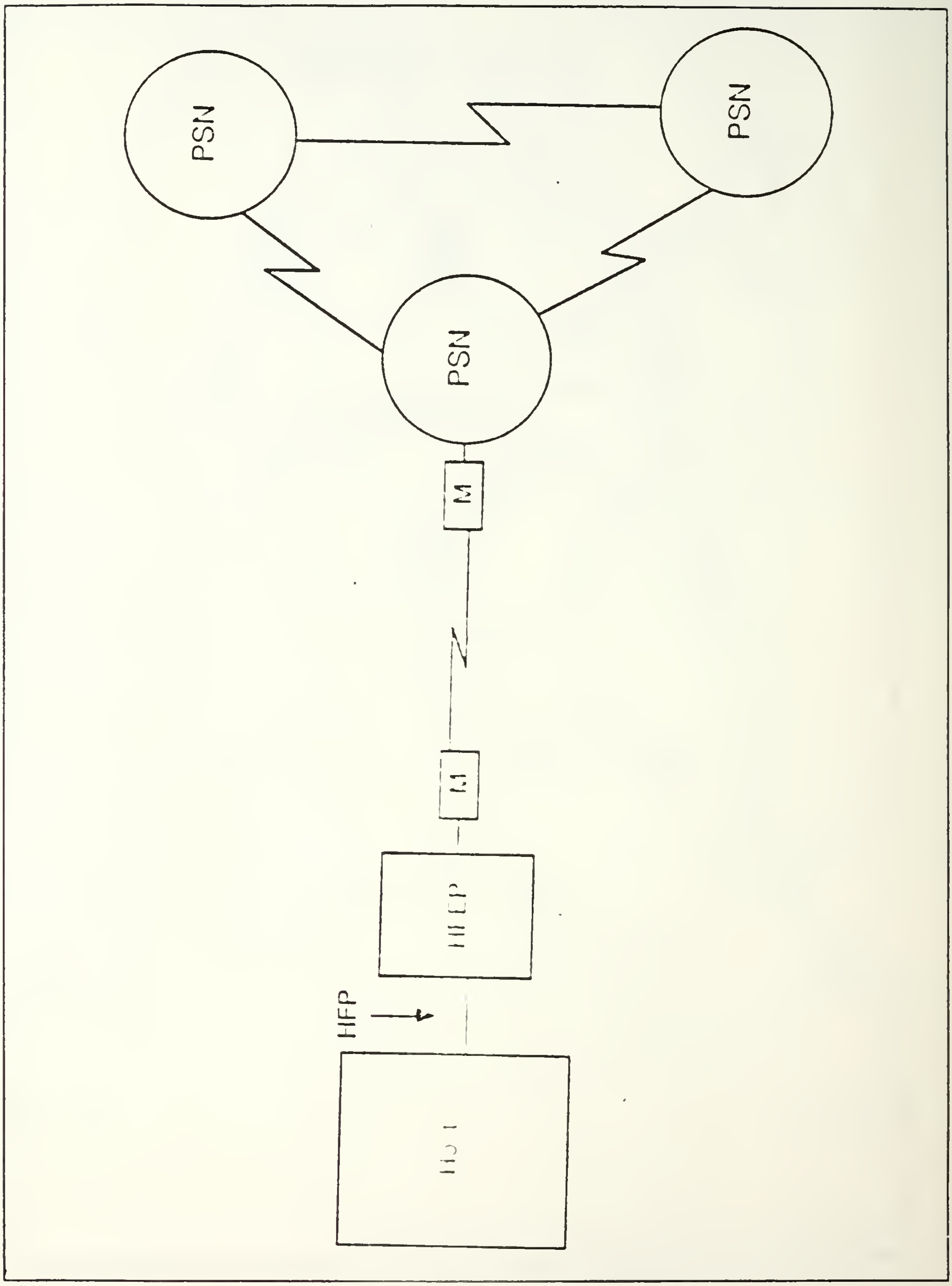


DYNAMIC ROUTING

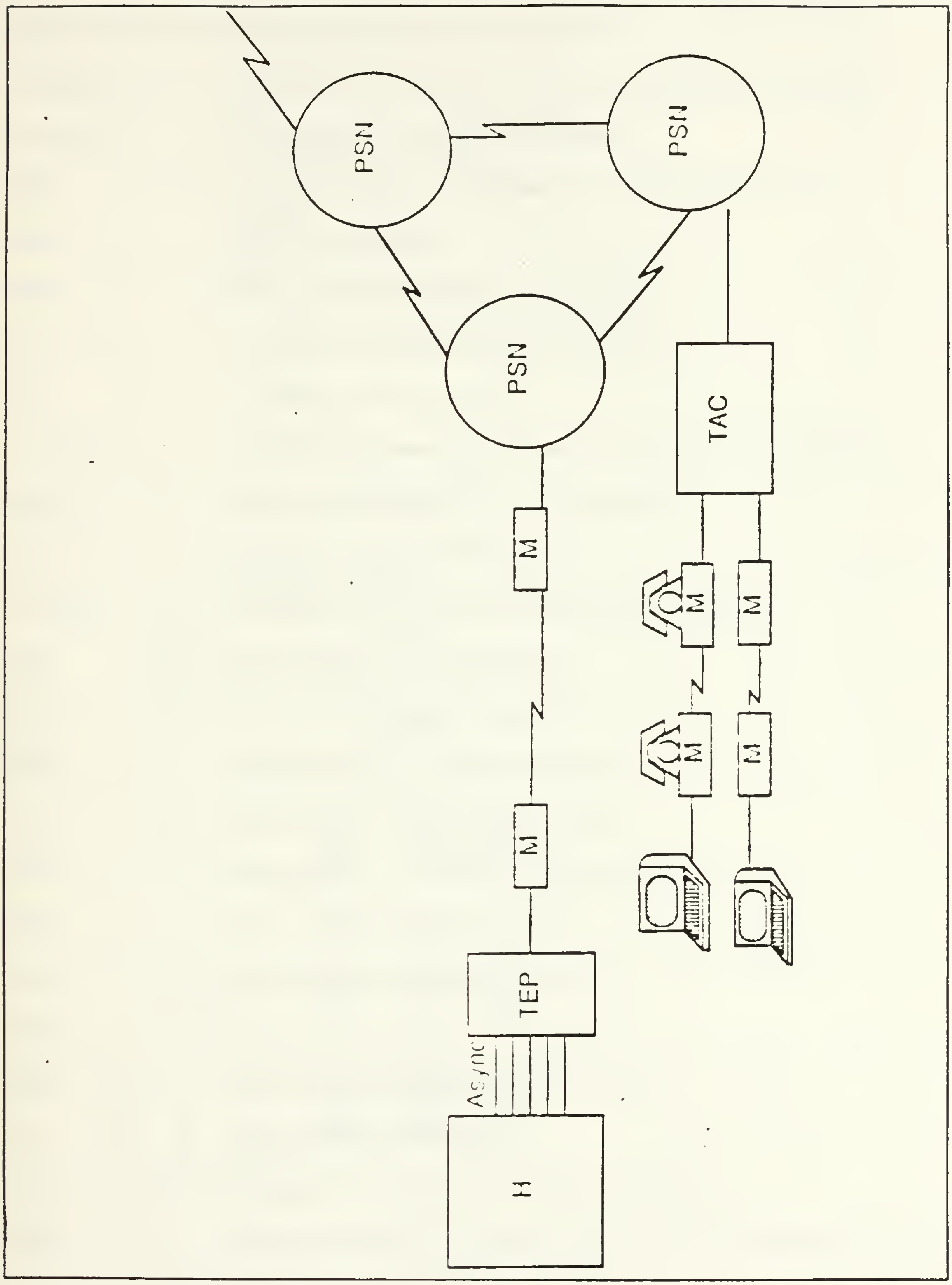


APPENDIX F

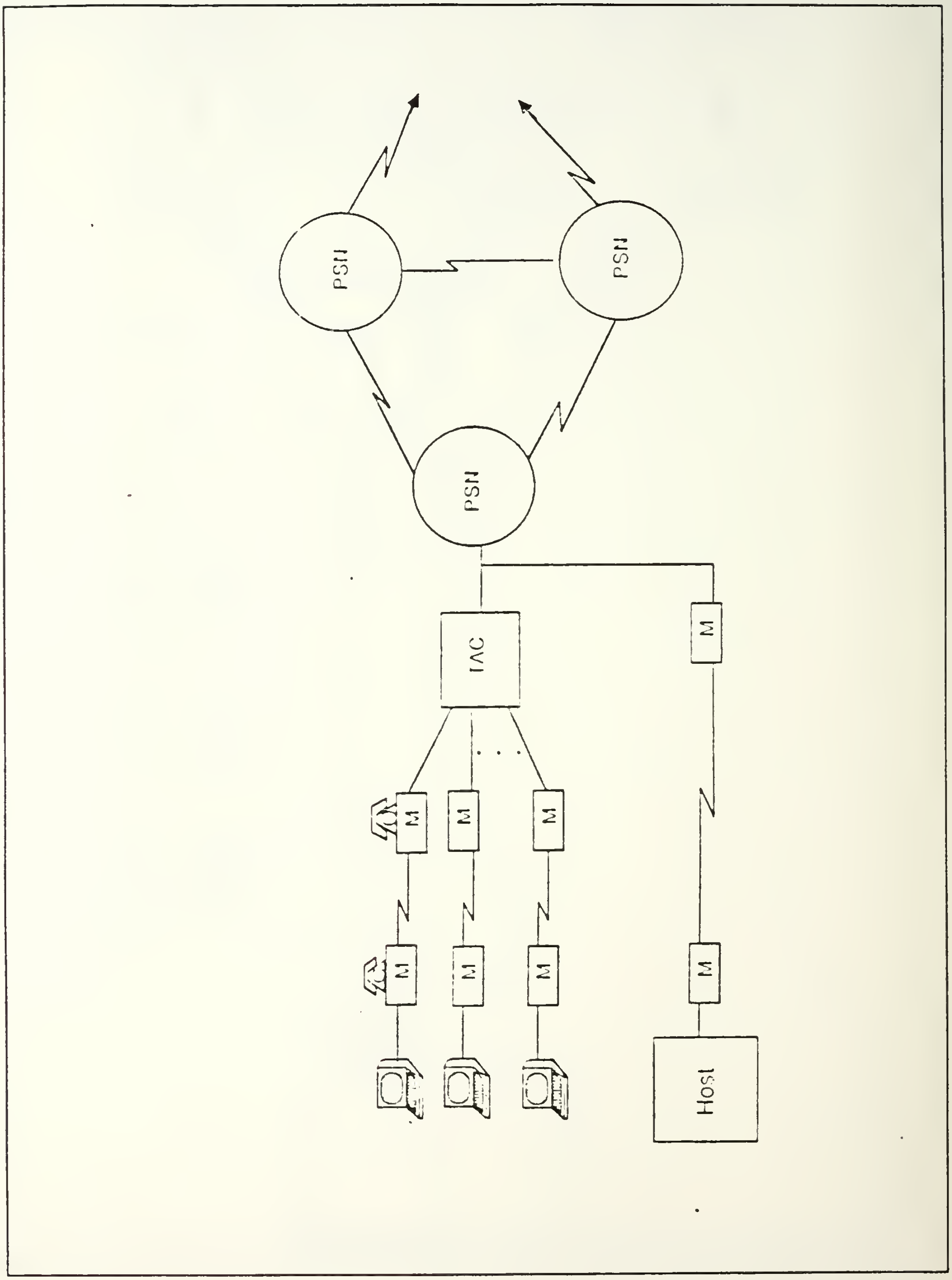
HOST FRONT END PROCESSOR



TERMINAL EMULATION PROCESSOR



TERMINAL ACCESS CONTROLLER



APPENDIX G

LIST OF ACRONYMS

ADP	Automated Data Processing
ARPANET	Advanced Research Projects Agency Network
AUTODIN	Automated Digital Network
BBN	Bolt Beranek and Newman, Incorporated
bps	bits per second
CATV	Community Antenna Television
CCU	Communications Control Unit
CRT	Cathode Ray Tube
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DDN	Defense Data Network
DISNET	Defense Integrated Secure Network
DOD	Department of Defense
DTE	Data Terminal Equipment
ECM	Electronic Countermeasure
EGP	Exterior Gateway Protocol
FDM	Frequency Division Multiplexing
FTP	File Transfer Protocol
GGP	Gateway-Gateway Protocol
HFEP	Host Front End Processor
IMP	Interface Message Processor
IP	Internet Protocol
IPLI	Internet Private Line Interface
ISO	International Organization for Standardization

IST	Inter-Switch Trunk
km	kilometer
MILNET	Military Network
MINET	Movement Information Network
NMC	Network Monitoring Center
NVT	Network Virtual Terminal
OSI	Open Systems Interconnection
PSN	Packet Switching Node
ROK	Republic of Korea
ROKM	Republic of Korea Military
SACDIN	Strategic Air Command Digital Network
SCINET	Sensitive Compartmented Information Network
SMTP	Simple Mail Transfer Protocol
TAC	Terminal Access Controller
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TEP	Terminal Emulation Processor
TN	Telnet
US	United States

LIST OF REFERENCES

1. Defense Communications Agency, Defense Data Network.

2. Sumner, M., Computers, Prentice-Hall, 1985.

3. Halsall, F., Introduction to Data Communications and Computer Networks, Addison-Wesley, 1985.

4. Stallings, W., Data and Computer Communications, Macmillan, 1985.

5. Brooks, C.H.P. and others, Information Systems Design, Prentice-Hall, 1982.

6. Vijay, A., Design and Analysis of Computer Communication Network, Mcgraw-Hill, 1982.

7. Defense Communications Agency, The DDN Course, April 1986.

8. Stallings, W., Local Networks: An Introduction, Macmillan, 1984.

9. Cerf, V.G. and Kahn, R.E., "A Protocol for Packet Network Intercommunication," IEEE Transactions on Communications, v. com-28, no. 4, April 1980.

10. Defense Communications Agency, Defense Data Network Program Plan, January 1982.

11. Cerf, V.G. and Kirstéin, P.T., "Issues in Packet-Network Interconnection," Proceedings of the IEEE, v.66, no. 11, November 1978.

12. Maybaum, F.L. and Duffield, H.C., Defense Data Network, An Overview, 1986.

13. Postel, J.B., ed., "DOD Standard Transmission Control Protocol," ACM Computer Communications Review, v. 10, no.4, October 1980.

14. Deputy Secretary of Defense Memorandum to Secretaries of the Military Departments, Defense Data Network Implementation, March 1983.

15. Defense Communications Agency, Defense Data Network Subscriber Interface Guide, July 1983.

16. US Department of Defense Military Standard MIL-STD-1782, Telnet Protocol Specification, August 1983.

17. US Department of Defense Military Standard MIL-STD-1780, *File Transfer Protocol*, September 1983.

18. Fidelman, M. R., Herman, J. G., and Baum, M. S., "Survivability of the Defense Data Network," *Signal*, May 1986.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Professor Judith H. Lind Code 55 Li Naval Postgraduate School Monterey, California 93943-5000	2
4.	Professor Dan C. Boger Code 54 Bo Naval Postgraduate School Monterey, California 93943-5000	1
5.	Library, P.O.Box 77 Gong Neung-Dong, Do Bong-Gu, Seoul 130-09 Republic of Korea	1
6.	Lee, Kyoo Won 120, Ho Myung-Ri, Kang Dong-Myun, Weol Sung-Gun, Kyung Buk-Do, Republic of Korea	10
7.	Park, Sang Chul SMC 2905 Naval Postgraduate School Monterey, California 93943	1
8.	Park, Nai Soo SMC 1831 Naval Postgraduate School Monterey, California 93943	1
9.	Park, Soon Sang SMC 2808 Naval Postgraduate School Monterey, California 93943	1
10.	Kim, Tae Woo SMC 2555 Naval Postgraduate School Monterey, California 93943	1

11. Kim, Yong Joo 1
SMC 1017
Naval Postgraduate School
Monterey, California 93943

12. Park, Hun Keun 1
SMC 2997
Naval Postgraduate School
Monterey, California 93943